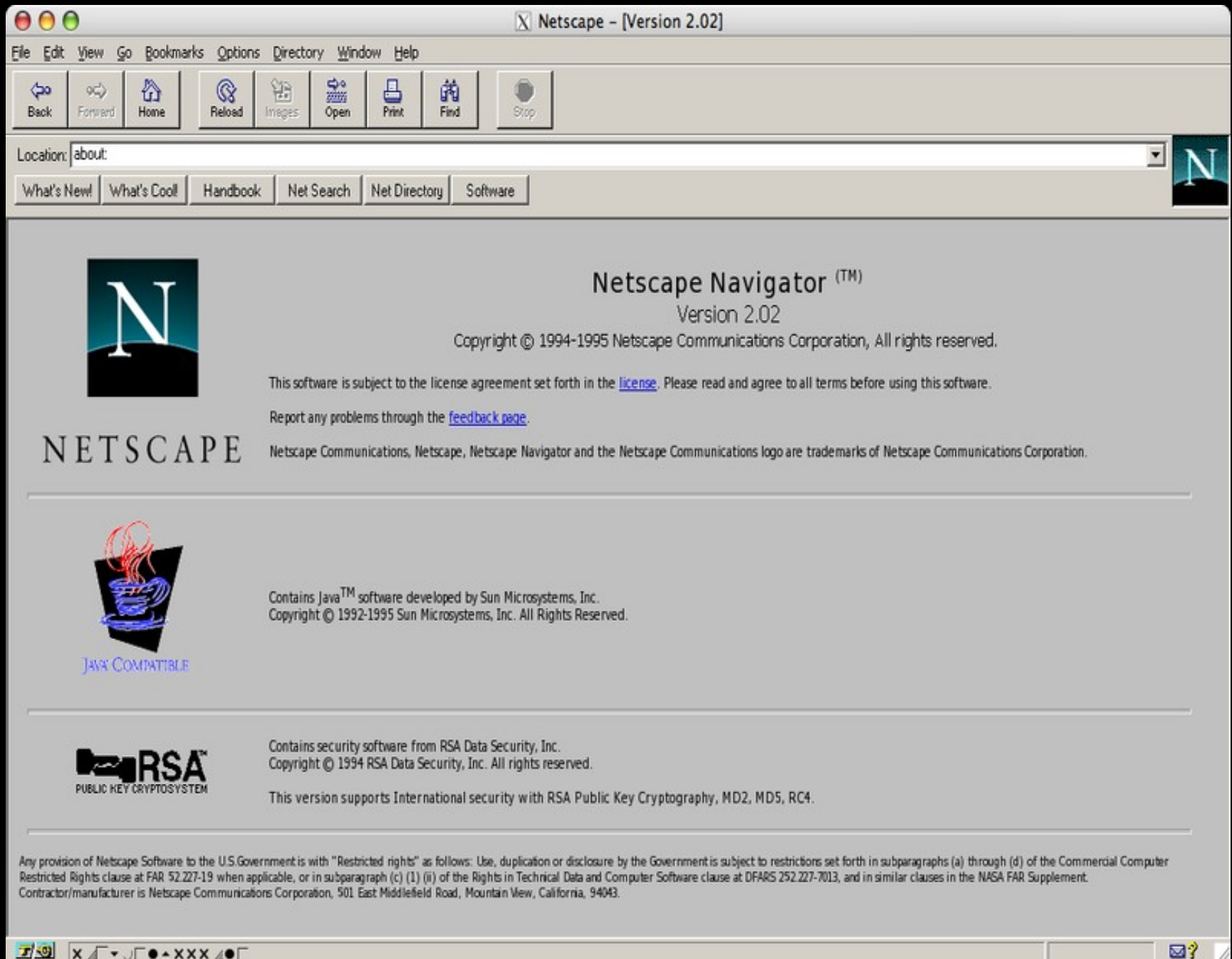
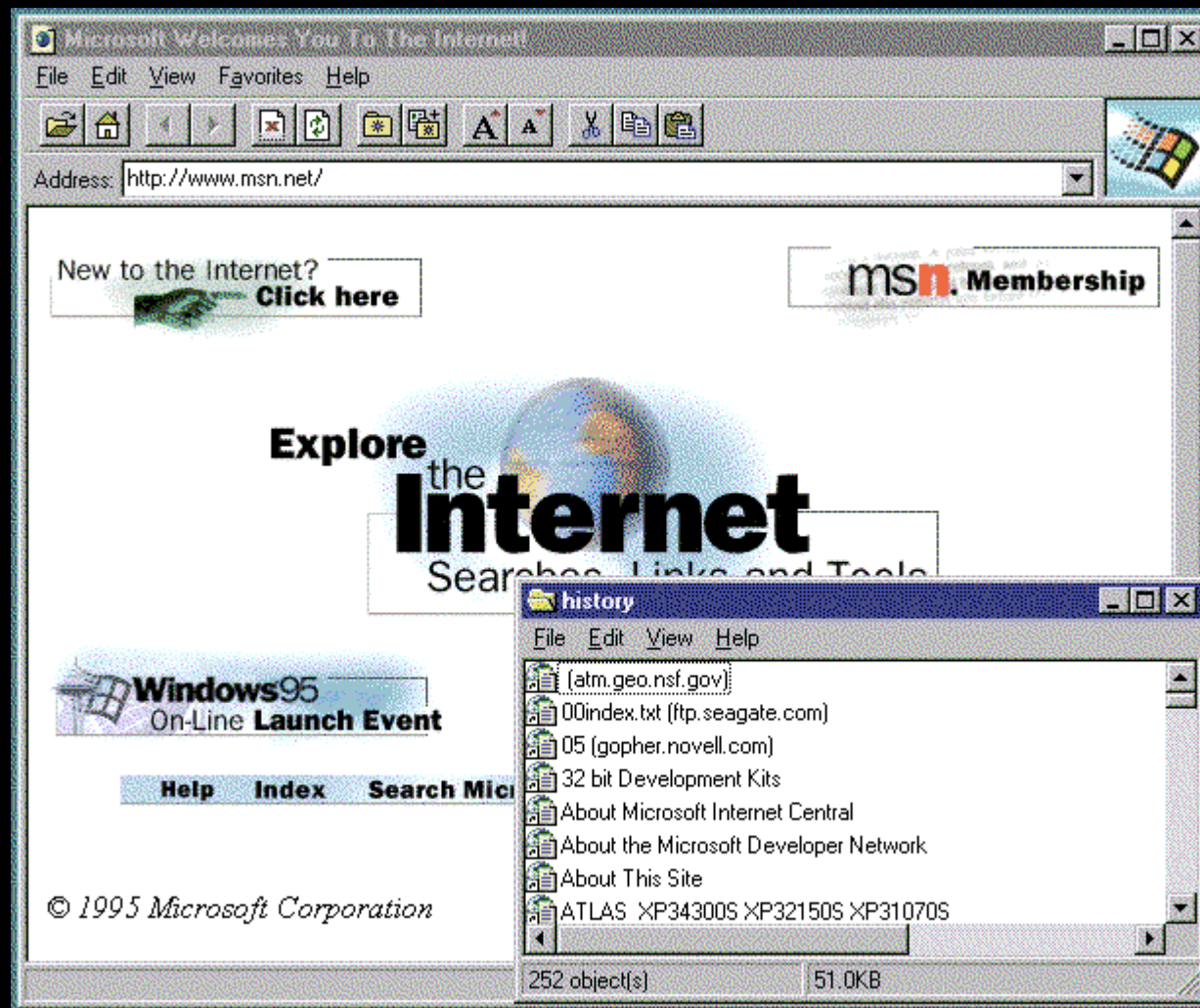


CHANGING THREATS TO PRIVACY

MOXIE@THOUGHTCRIME.ORG









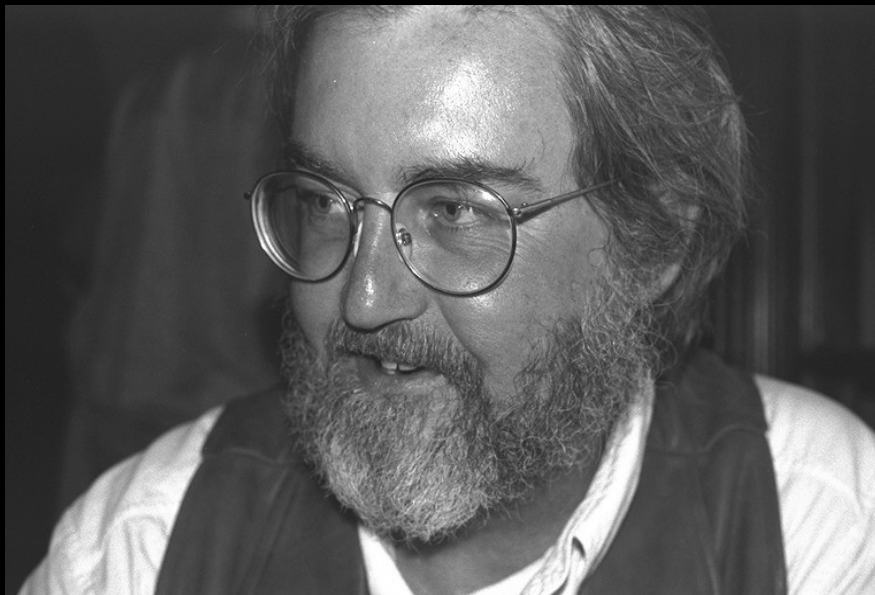






CYPHERPUNKS

GOVERNMENT



DANGEROUS

SCARED

THE FUCK

OUT OF THEM

ULTIMATE CONTROL → No CONTROL

AS DANGEROUS?



=

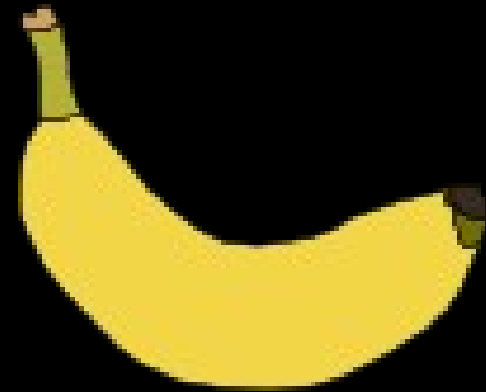




CRYPTOGRAPHY IS NOT A BANANA



!=



CYPHERPUNKS WRITE CODE!



“PGP: SOURCE CODE AND INTERNALS”
MIT PRESS 1995

2000 == GAME OVER?

THE SPREAD OF INFORMATION IS
INEVITABLE

PREDICTIONS

- Anonymous digital cash will flourish.
- Intellectual property will disappear.
- Surveillance will become impossible.
- Governments will be unable to continue collecting taxes.
- Governments will fall.

10 YEARS ON

Amazon.com: Going Rogue: An American Life (9780061939891): Sarah Palin: Books - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.amazon.com/Going-Rogue-American-Sarah-Palin/dp/0061939897/

Most Visited Getting Started Latest Headlines

Amazon.com: Going Rogue: An ...

amazon.com Hello. Sign in to get personalized recommendations. New customer? Start here. FREE 2-Day Shipping, No Minimum Purchase: See details

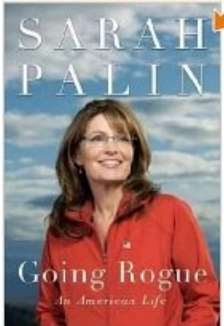
Your Amazon.com Today's Deals Gifts & Wish Lists Gift Cards Your Account Help

Shop All Departments Search Books GO Cart Wish List

Books Advanced Search Browse Subjects New Releases Bestsellers The New York Times® Bestsellers Libros En Español Bargain Books Textbooks

Going Rogue and over 420,000 other books are available for Amazon Kindle – Amazon's new wireless reading device. Learn more

Click to LOOK INSIDE!



Going Rogue: An American Life (Hardcover)
~ Sarah Palin (Author)
★★★★☆ (1,220 customer reviews)

List Price: ~~\$28.99~~
Price: **\$13.50** & eligible for **FREE Super Saver Shipping** on orders over \$25.
[Details](#)
You Save: **\$15.49 (53%)**

In Stock.
Ships from and sold by Amazon.com. Gift-wrap available.

Want it delivered **Friday, February 26?** Order it in the next **0 hours and 23 minutes**, and choose **One-Day Shipping** at checkout. [Details](#)

[113 new](#) from \$7.94 [57 used](#) from \$8.22 [12 collectible](#) from \$18.99

Formats	Amazon Price	New from	Used from
Kindle Edition	\$9.99	--	--
Hardcover	\$13.50	\$7.94	\$8.22
Paperback, Large Print	\$19.13	\$15.71	\$15.71
Audio, CD, Abridged, Audiobook	\$19.79	\$16.18	\$16.12
Audio, Download	\$15.74 or less with new Audible membership		

See all 16 customer images
Share your own customer images
[Search inside this book](#)

Start reading *Going Rogue* on your Kindle in under a minute.
Don't have a Kindle? [Get your Kindle here.](#)

Quantity: 1

Add to Cart

or

[Sign in](#) to turn on 1-Click ordering.

or

Add to Cart with FREE Two-Day Shipping

Amazon Prime Free Trial required. Sign up when you check out. [Learn More](#)

Add to Wish List

Express Checkout with PayPhrase

Persistent Tenderness

[What's this?](#) [Create PayPhrase](#)

More Buying Choices

[182 used & new](#) from \$7.94

Have one to sell? [Sell yours here](#)

Share

IS THIS VICTORY?

- Everyone's mother has an illegal copy of an mp3 somewhere.
- Cryptography is everywhere.
- There are actual darknets which should make the eradication of information impossible.

SURVEILLANCE > PRIVACY

WHAT HAPPENED?

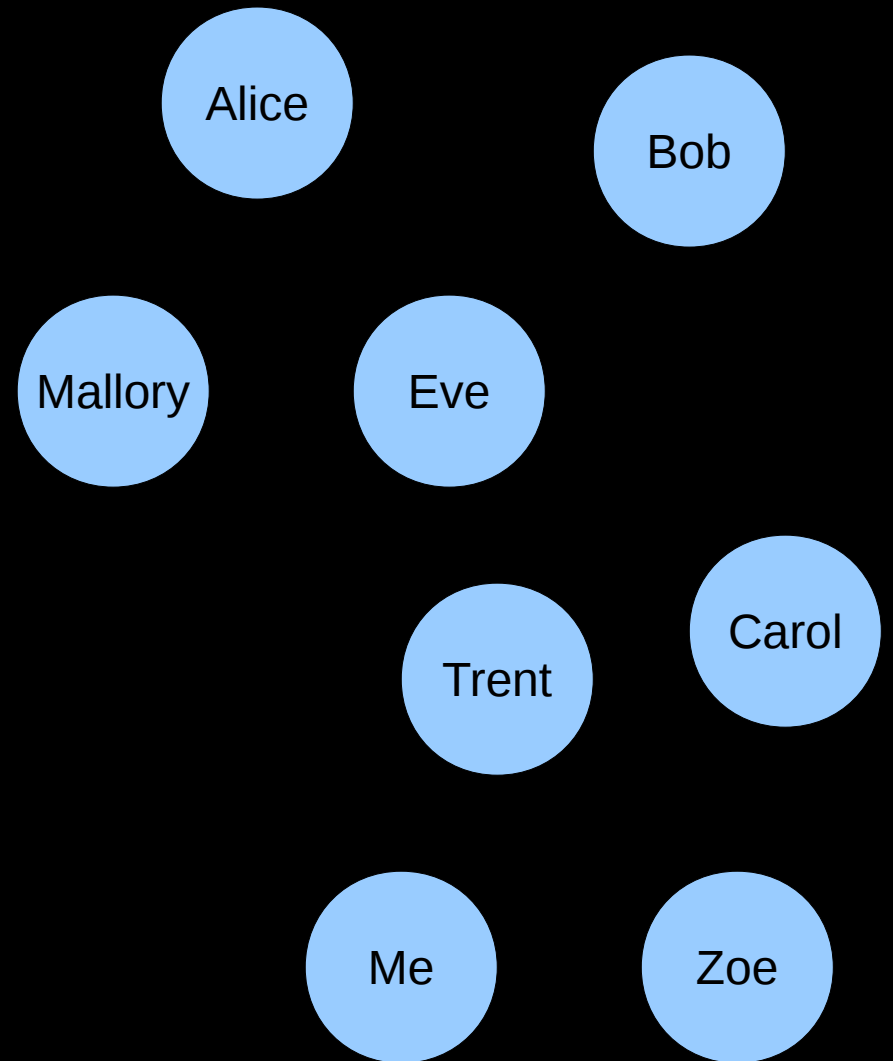
FUTURE

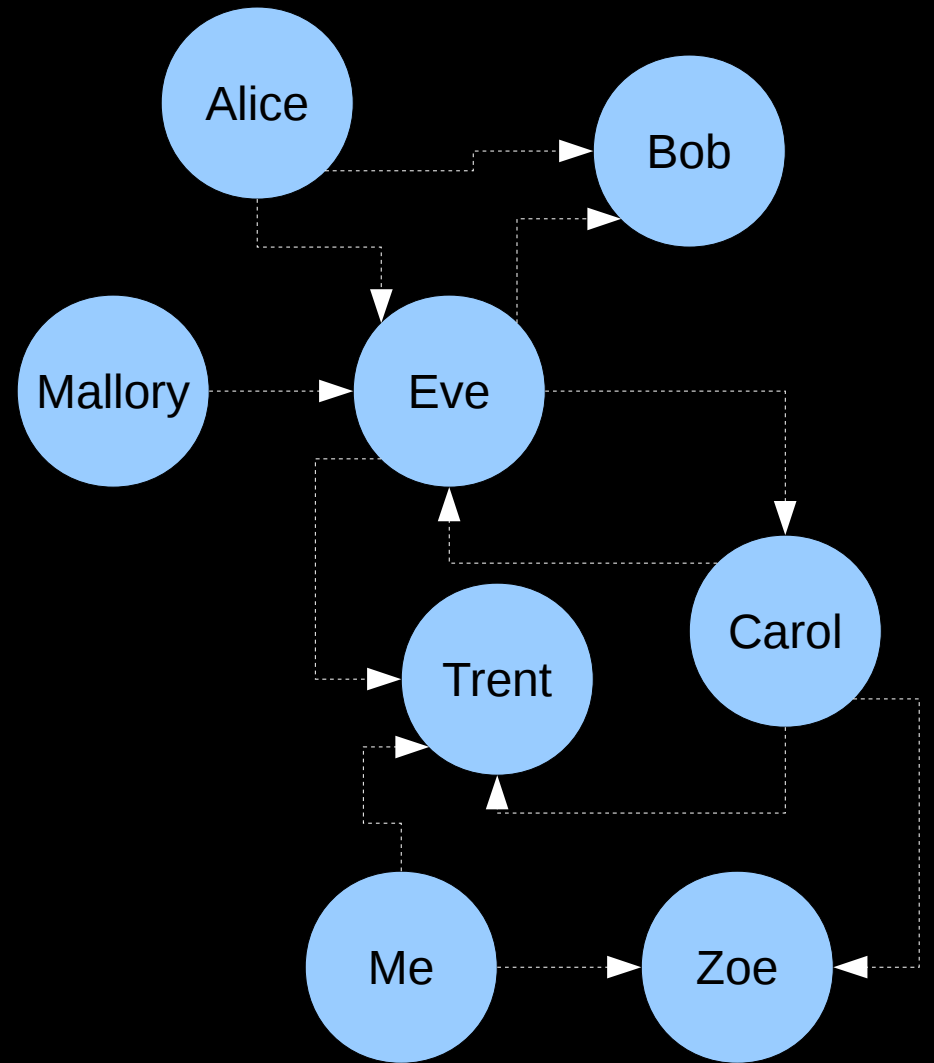
FACISM

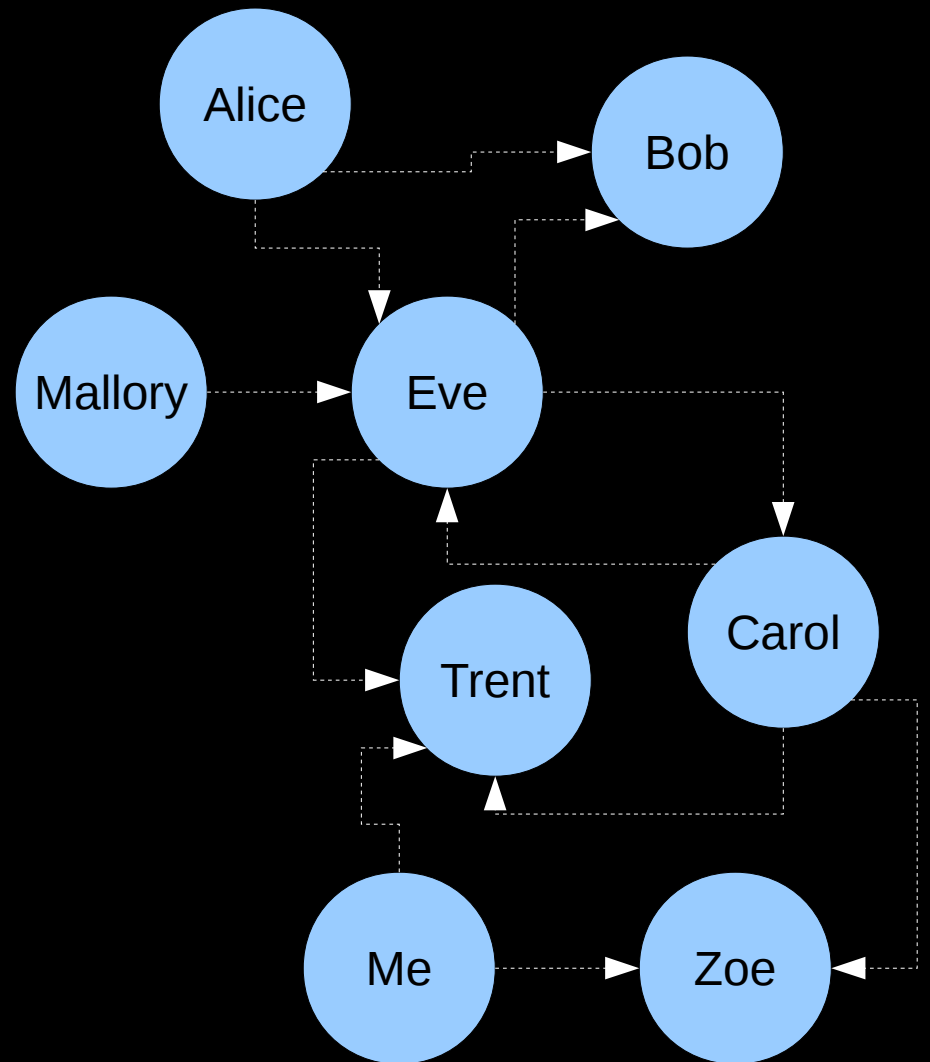
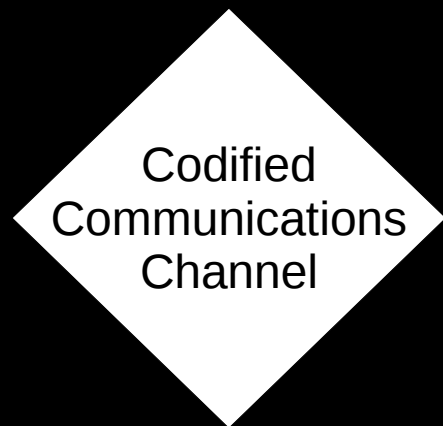
SOCIAL DEMOCRACY

CHOICE

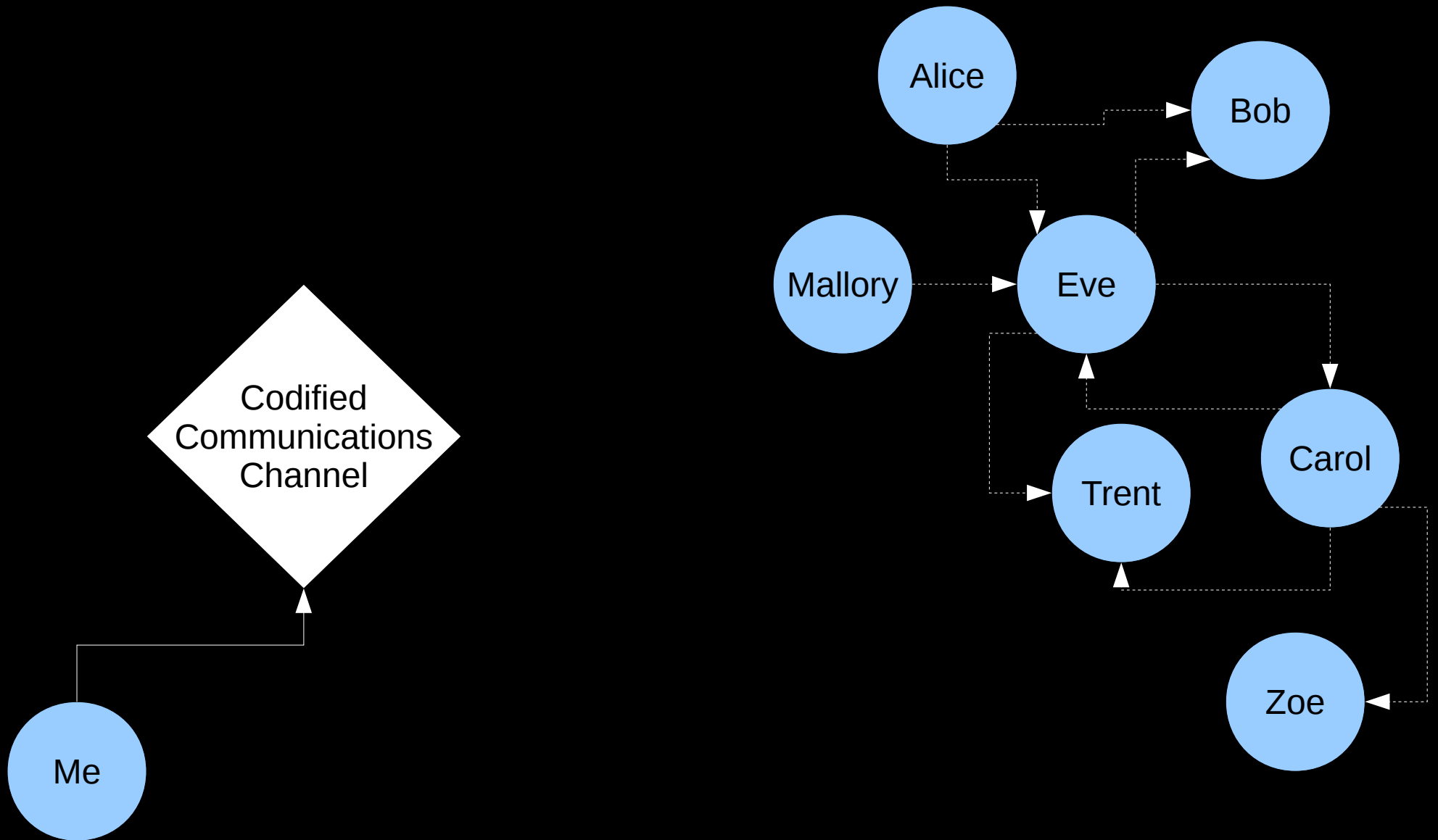


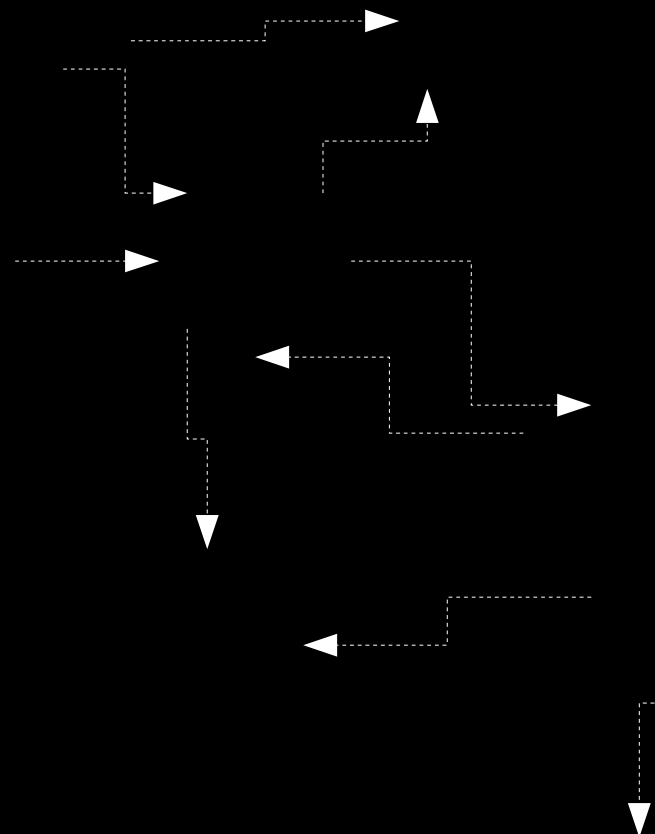
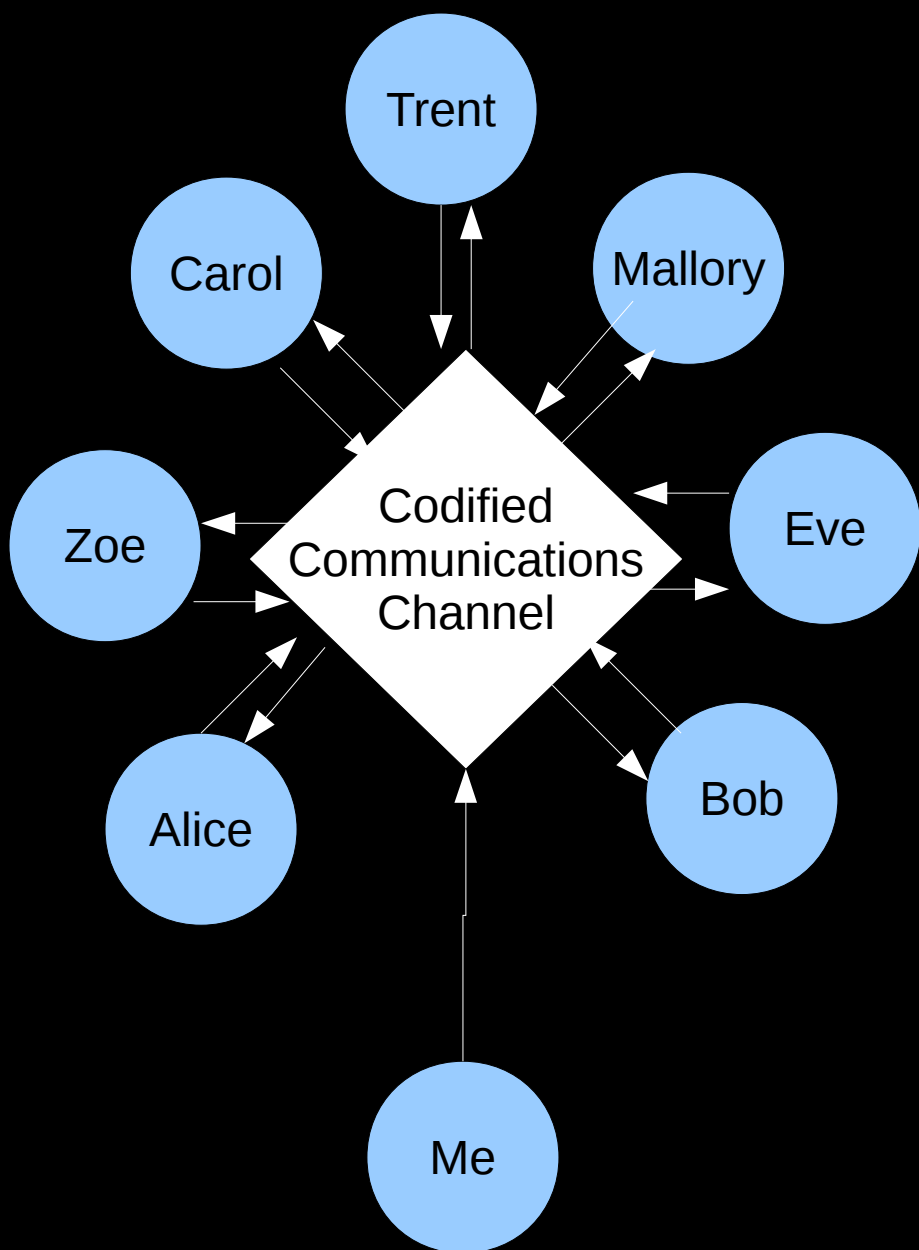


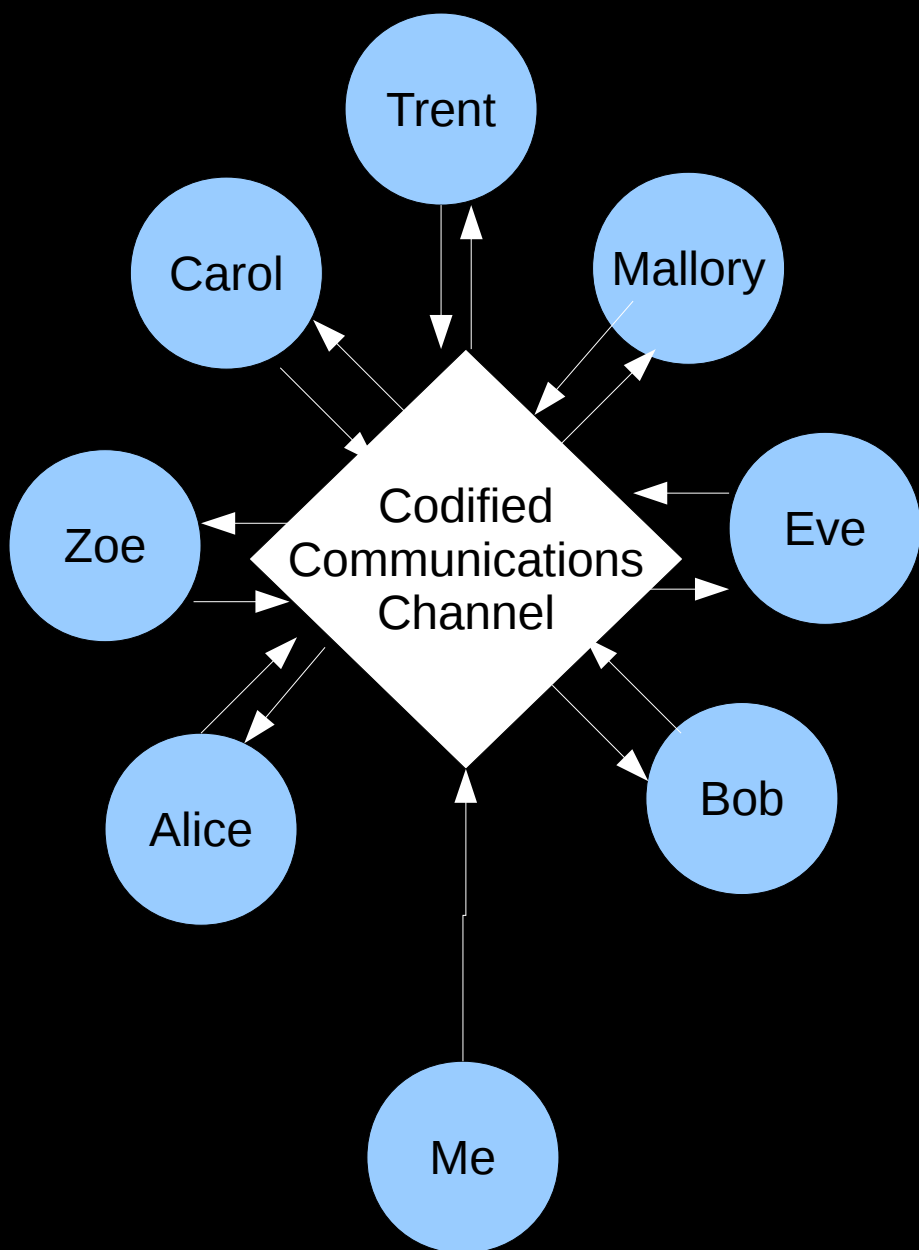




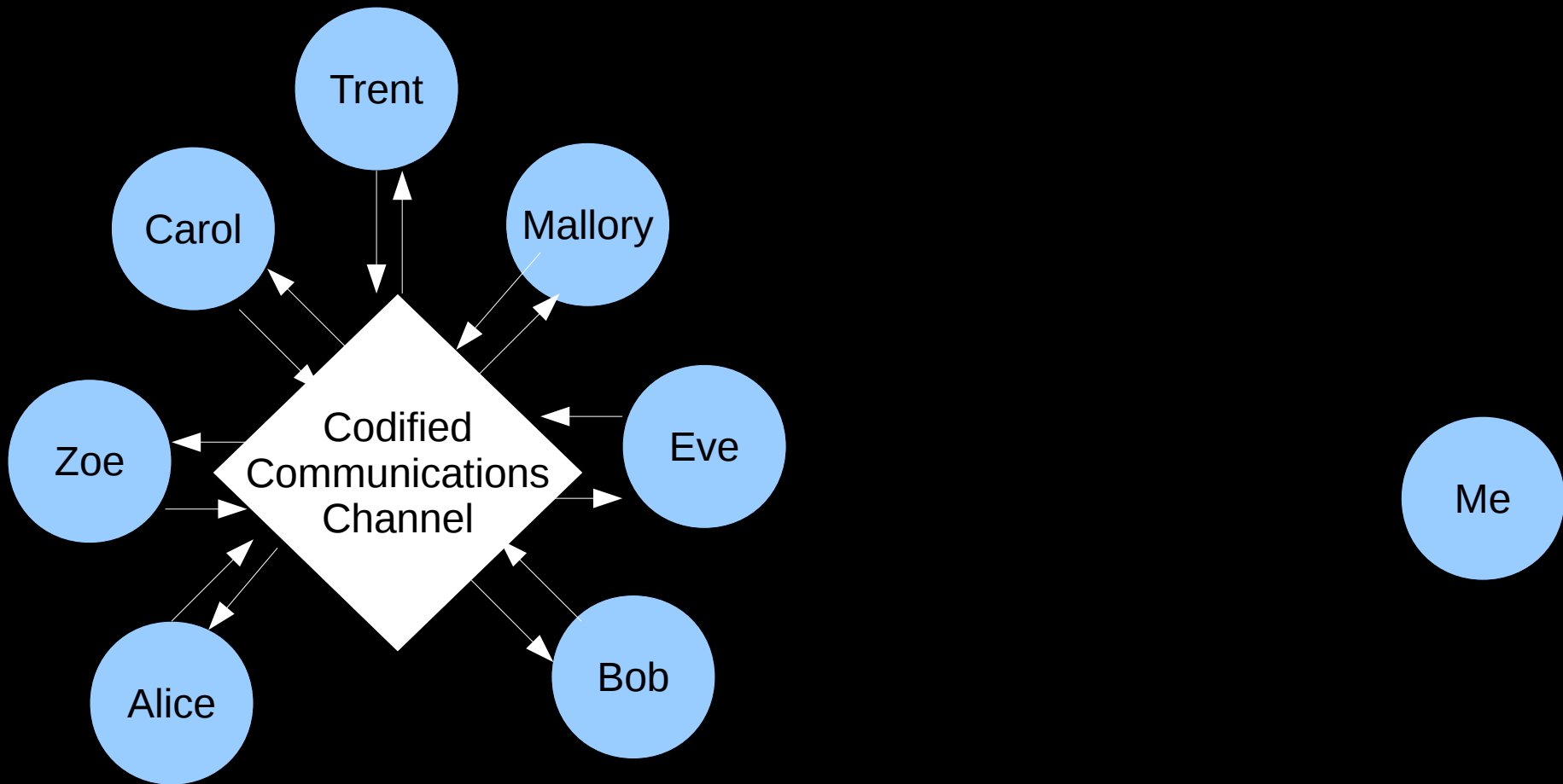
“NO NETWORK EFFECT”





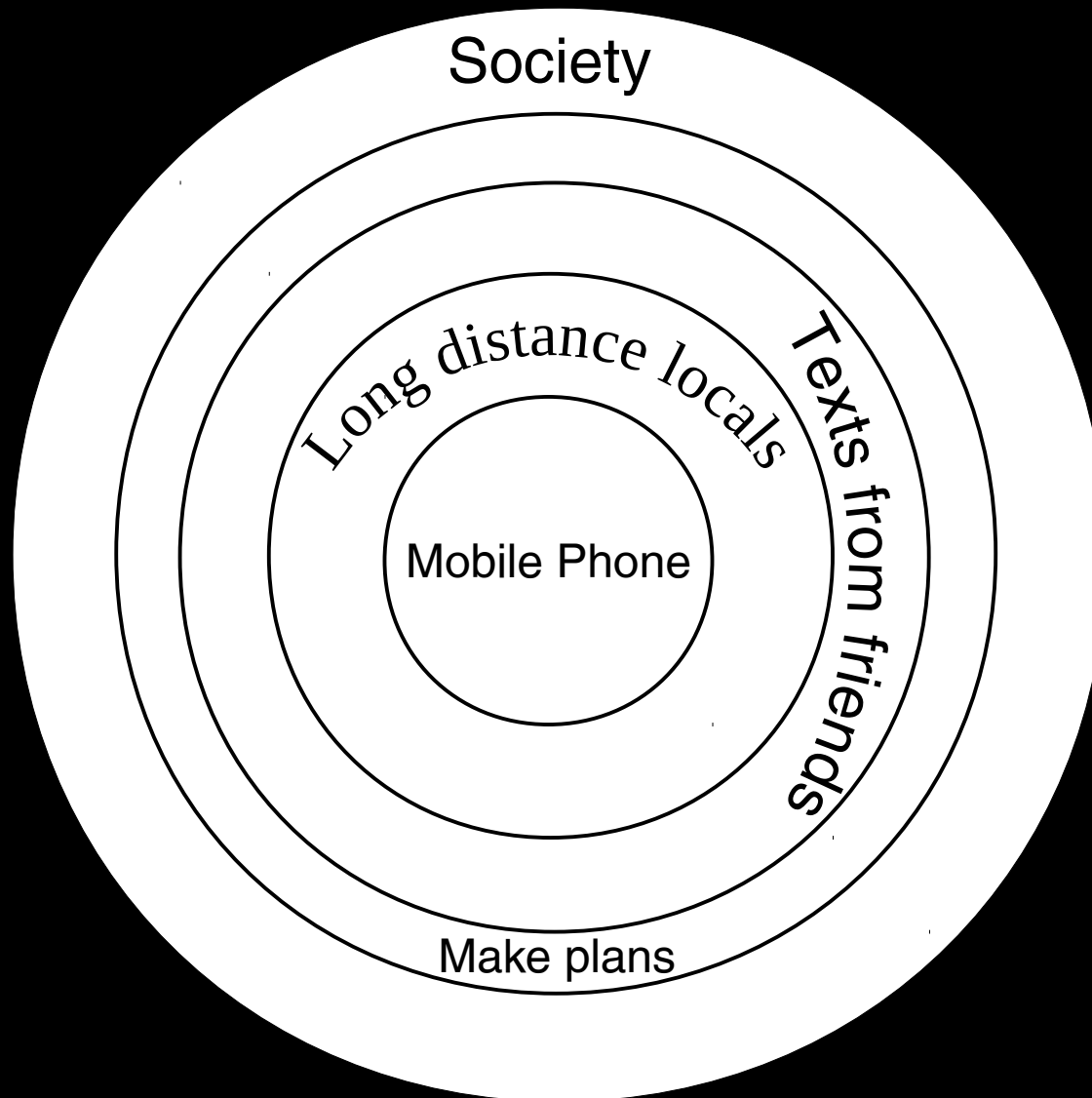


“NO NETWORK EFFECT”

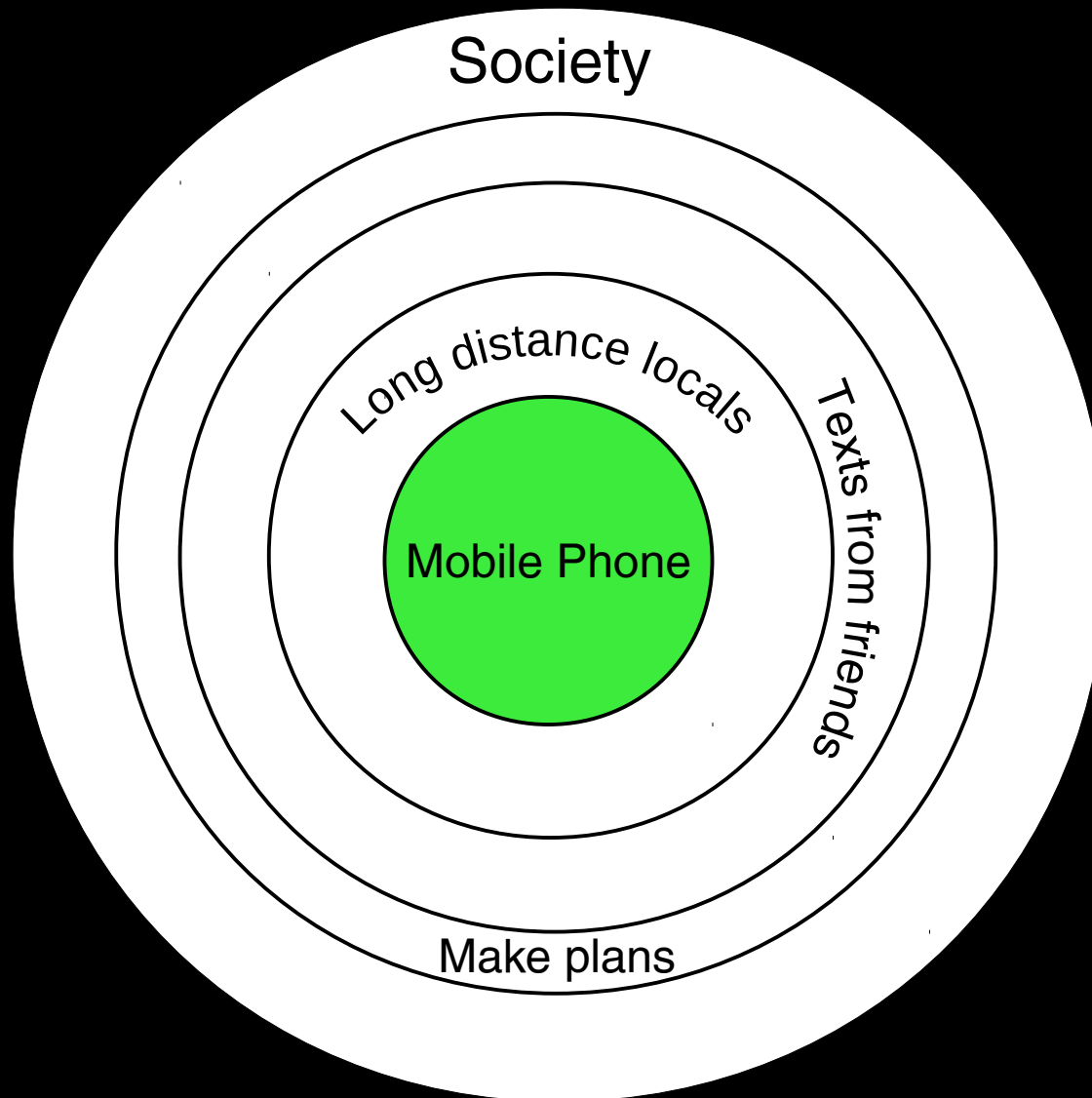


WHAT *kind* OF CHOICE?

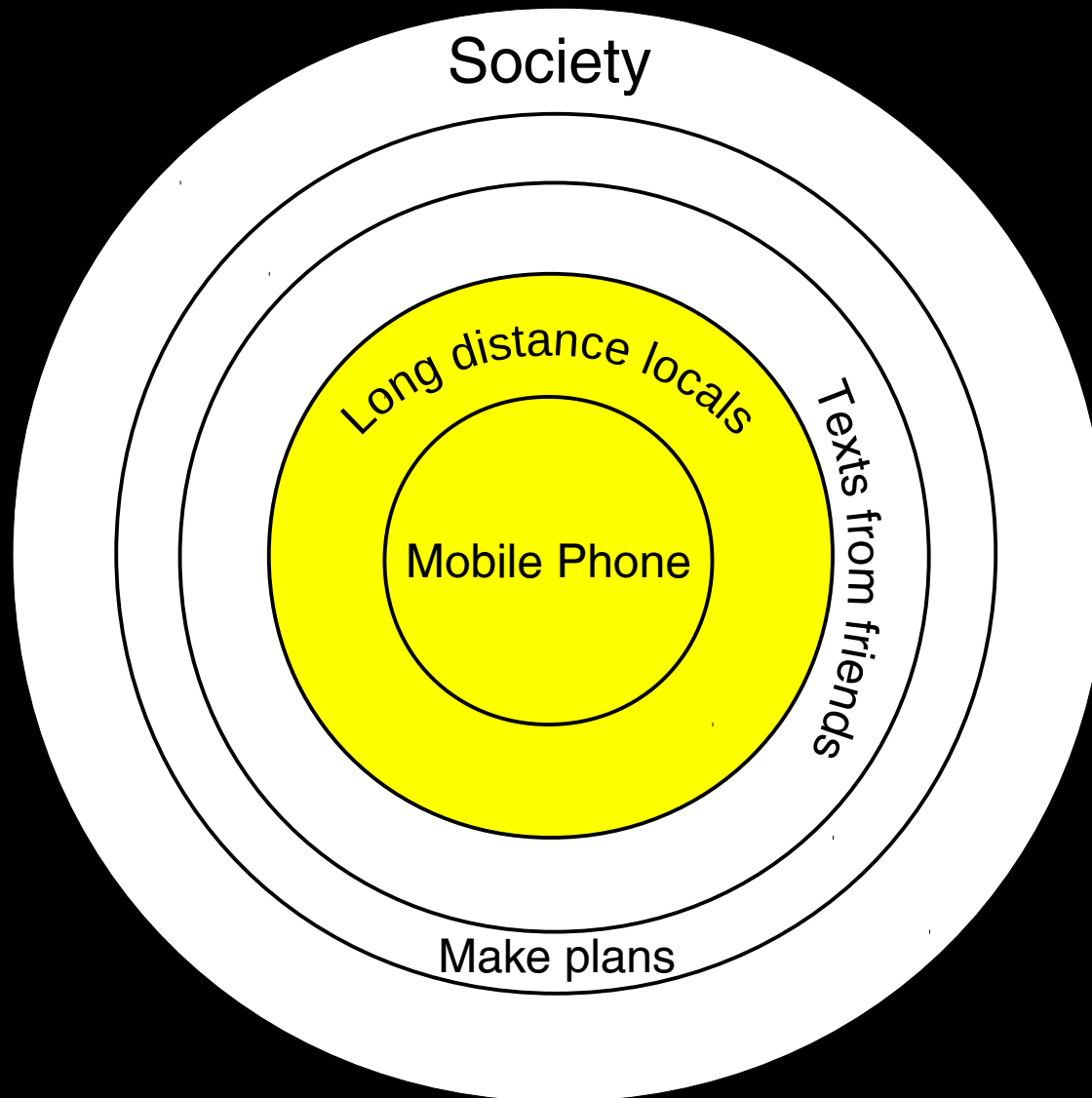
THE PUSH TO EXPAND CHOICE SCOPE



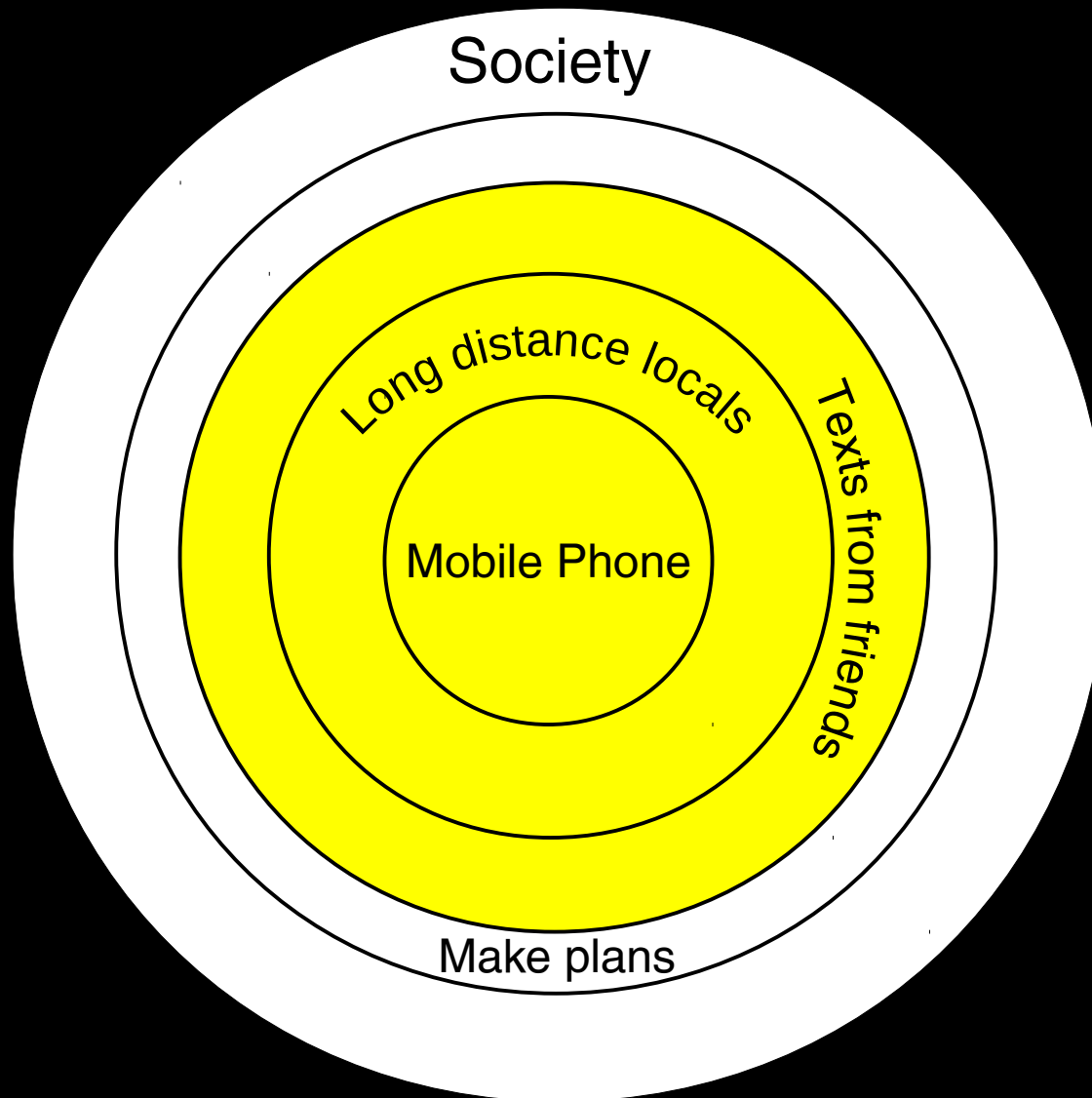
THE PUSH TO EXPAND CHOICE SCOPE



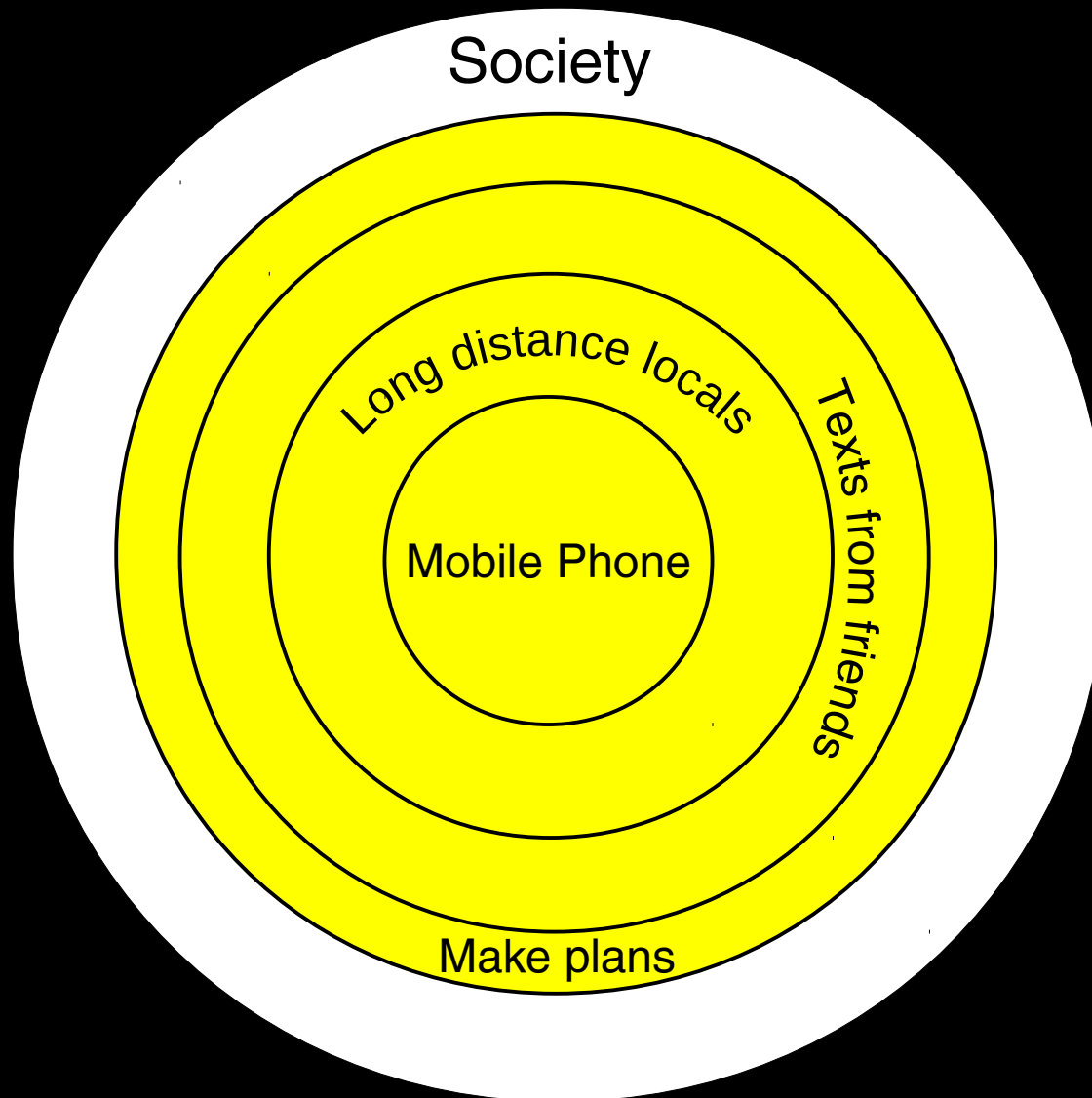
THE PUSH TO EXPAND CHOICE SCOPE



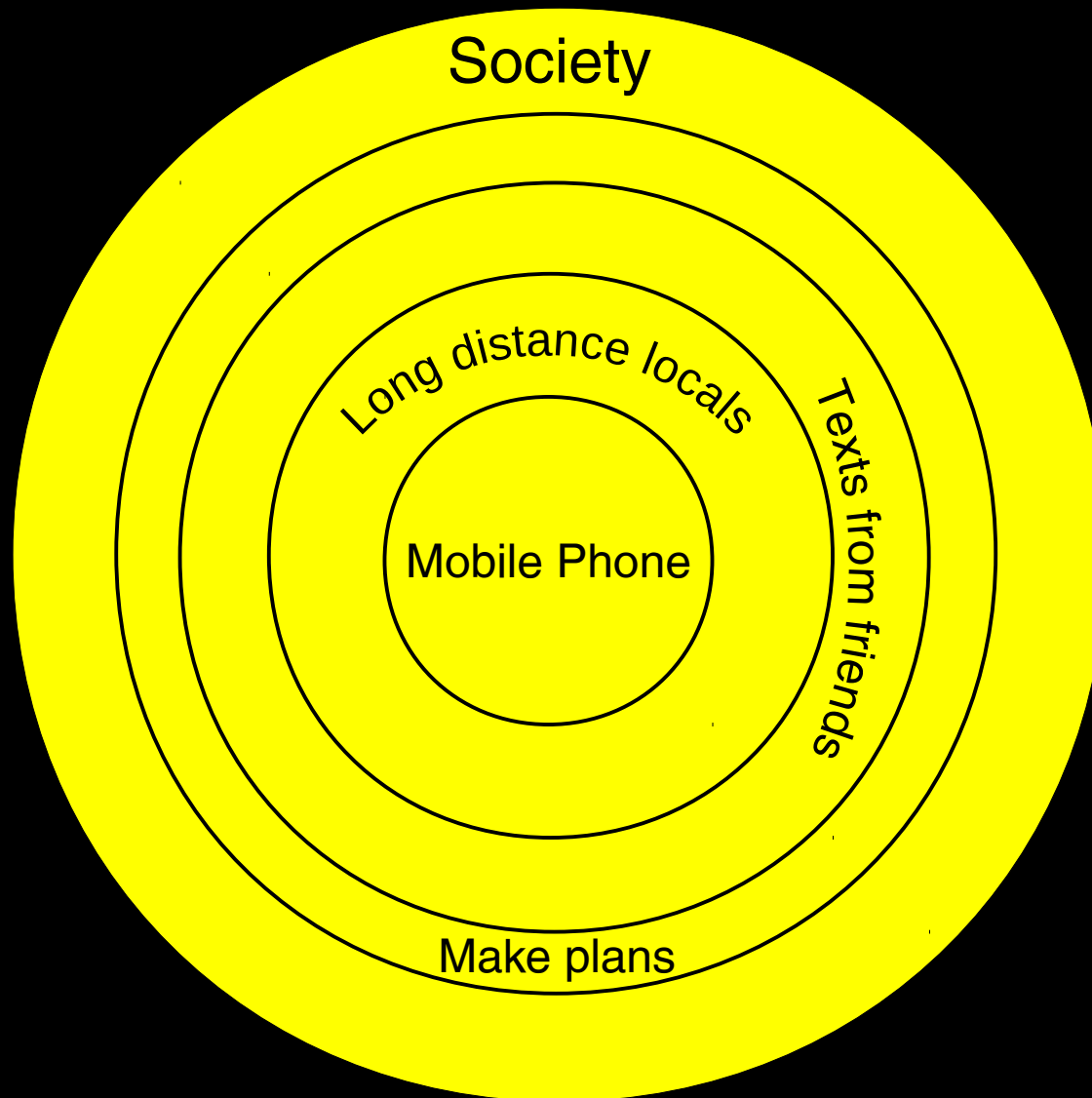
THE PUSH TO EXPAND CHOICE SCOPE



THE PUSH TO EXPAND CHOICE SCOPE



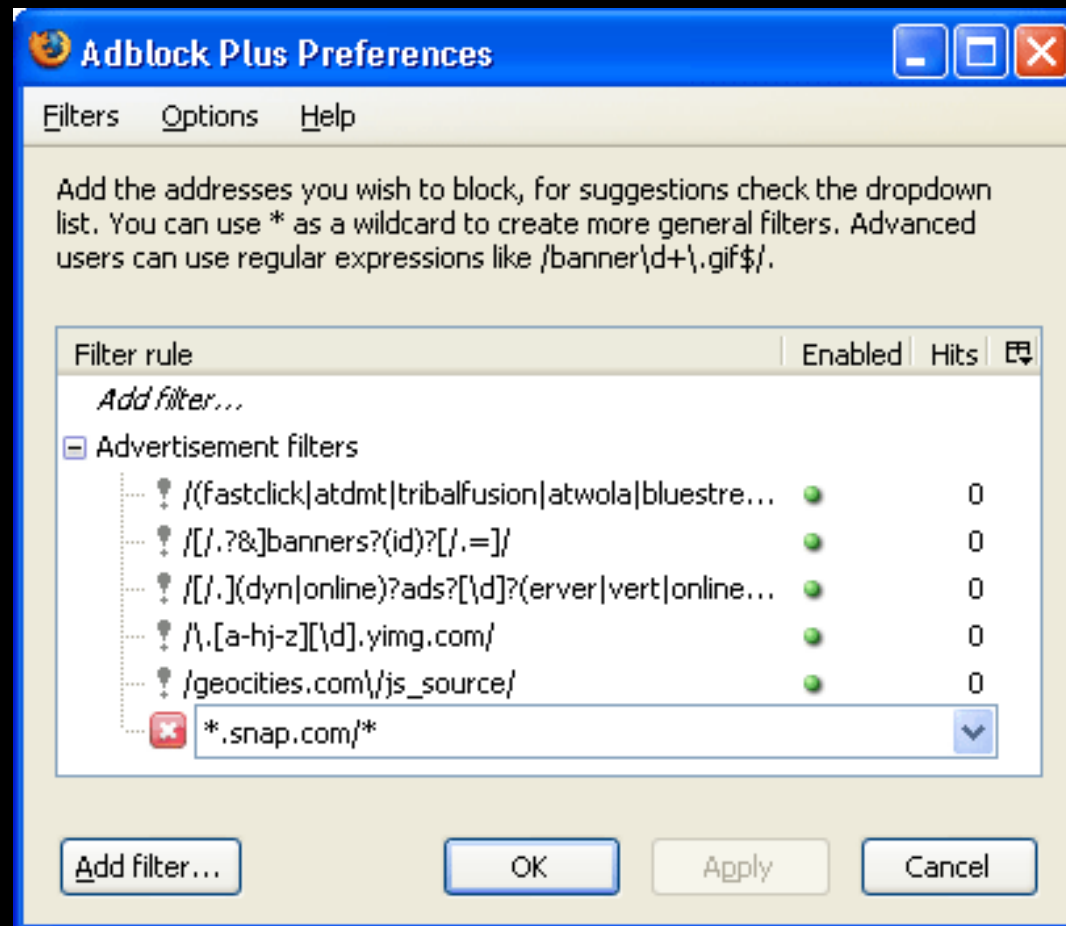
THE PUSH TO EXPAND CHOICE SCOPE



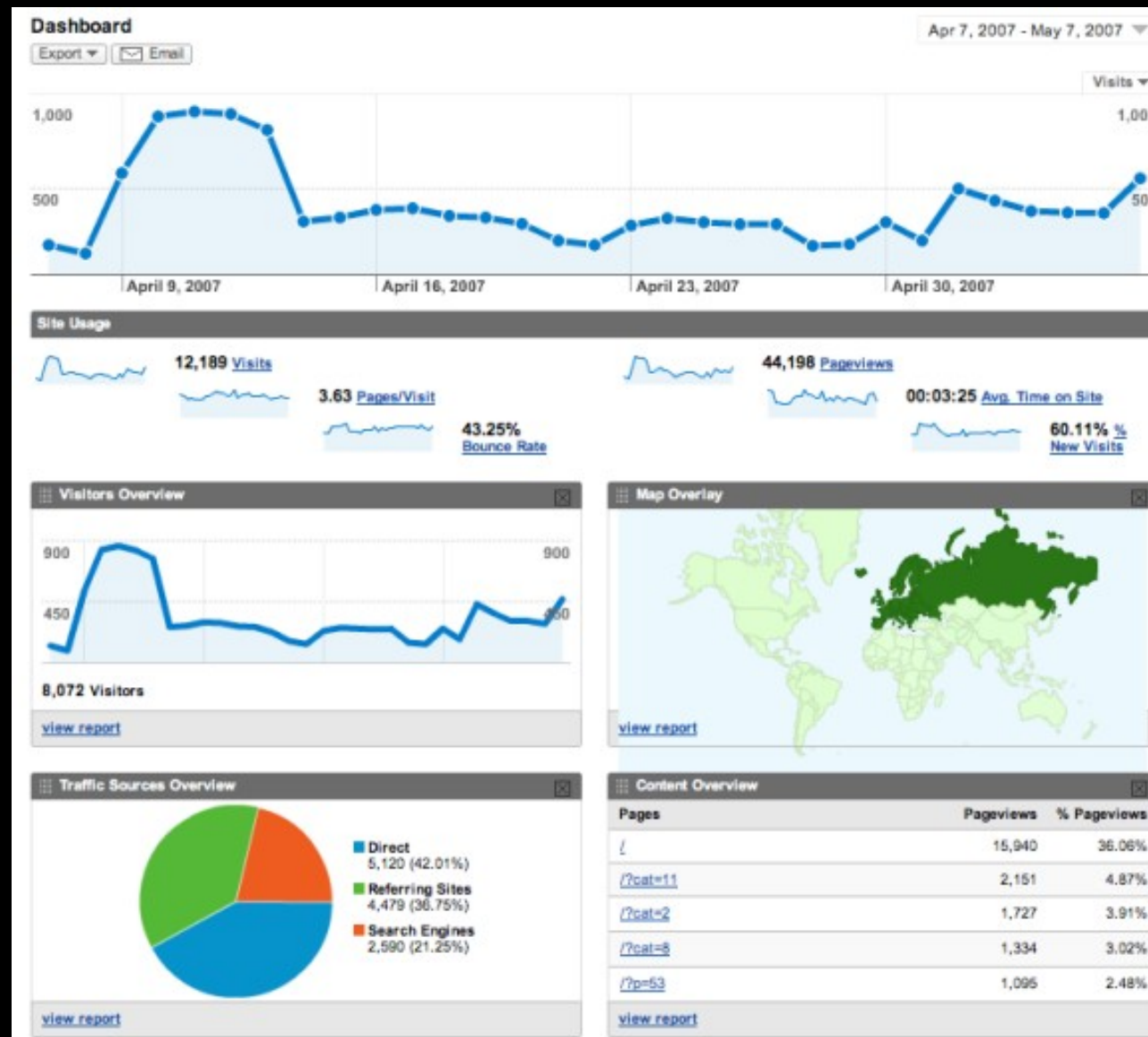
SMALL CHOICES → BIG CHOICES

EVERYWHERE

ANOTHER EXAMPLE



ANOTHER EXAMPLE



GOOGLE ANALYTICS == NOT EVIL?

ANOTHER EXAMPLE

```
<!-- BEGIN google analytics -->
<script type="text/javascript">
  var gaJsHost = (("https:" == document.location.protocol) ?
  "https://ssl." : "http://www.");
  document.write(unescape("%3Cscript src='" + gaJsHost +
  "google-analytics.com/ga.js' type='text/javascript'%3E%3C
  /script%3E"));
</script>
<script type="text/javascript">
  var pageTracker = _gat._getTracker("UA-30775-6");
  pageTracker._setDomainName("twitter.com");
  url = '/statuses/rebeccakelley/1207938518';
  pageTracker._setVar('Logged In');
  pageTracker._setVar('lang: en');
  pageTracker._trackPageview(url);
</script>

<!-- END google analytics -->
```

EXPAND THE SCOPE OF THE CHOICE

SIGNIFICANT?



Moxie Marlinspike
Institute For Disruptive Studies





TOTAL INFORMATION AWARENESS

“...data must be made available in large-scale repositories with enhanced semantic content for easy analysis...”

-John Poindexter

A SYSTEM FOR EASY DATA MINING

- Store all:
 - Email
 - Web Traffic
 - Credit Card History
 - Medical Records
- Develop the technology to easily mine the massive amount of data you collect.

THE TOTALITARIAN FUTURE, THE CYPHERPUNK NIGHTMARE

PEOPLE FREAKED OUT

PEOPLE FREAKED OUT



PEOPLE FREAKED OUT



PEOPLE FREAKED OUT



PEOPLE FREAKED OUT



A SYSTEM FOR EASY DATA MINING

- Store all:

- Email —————→
- Web Traffic —————→
- Credit Card History —→
- Medical Records —————→



- Develop the technology to easily mine the massive amount of data you collect.
 - That's Google's jam!

INTENT

SURVEILLANCE BUSINESS

EFFECT IS THE SAME

Who knows more about the citizens in their own country, Kim Jong-Il or Google?

CHOICE

THE CHOICE IS EXPANDING

SOCIETY

TRENDS HAVE CHANGED

- Technology alters society.
- Information accumulates in distinct places as a result.
- Eavesdroppers move to those points of accumulation.

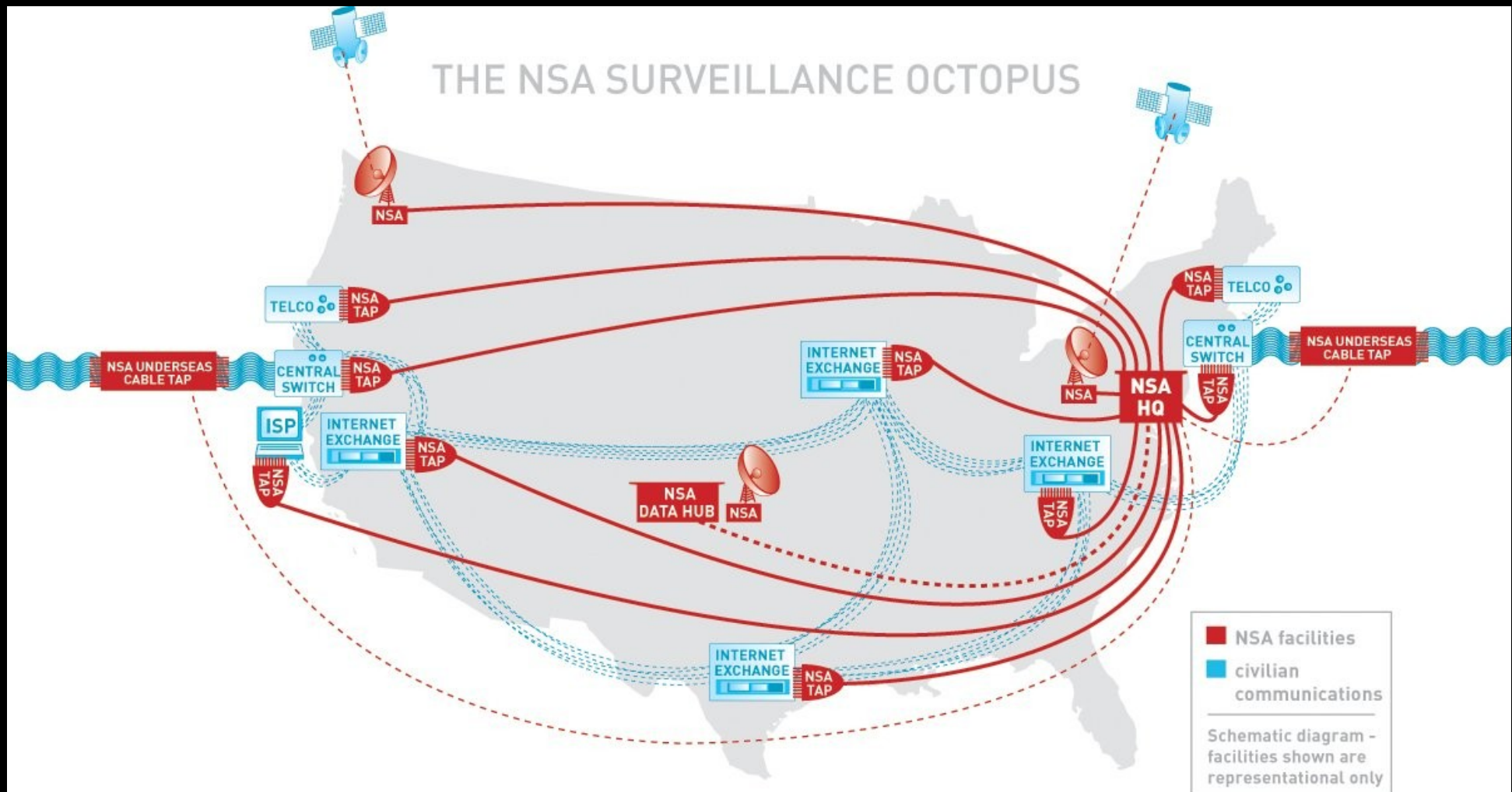
PAST WAS DIRECT

PAST



PRESENT IS SUBTLE

PRESENT



PRESENT



PAST WAS DIRECT



PRESENT IS SUBTLE

The Google logo, featuring the word "Google" in its signature multi-colored font (blue, red, yellow, blue, green, red) with a trademark symbol (TM) to the upper right.The Twitter logo, featuring the word "twitter" in a light blue, rounded, lowercase font with a white outline.The Facebook logo, featuring the word "facebook" in white, lowercase, sans-serif font on a dark blue rectangular background.

THOUGHTS FOR THE FUTURE

1. Deal with the choices that aren't choices.

ACKNOWLEDGE

CHOICES → EXPANDING

CHOICES → DEMANDS

SOME PROJECTS

WHAT'S UP WITH GOOGLE?

- They have an awful lot of data.
 - They record everything. Your IP address, the cookie they issue, your search requests, the contents of every email you've sent or received, the news you read, the places you go, even your TCP headers. They're even collecting realtime GPS location and DNS lookups.
 - They know who your friends are, where you live, where you work, and where you spend your free time. They know about your health, your love life, and your political leanings.
 - They know not just what you're *doing*, but also a lot about what you're *thinking*.

CONTROL THE TERMS

- “We anonymize your data after nine months.”
 - “Anonymize” means drop the last octet of an IP address. And cookies are simply translated.
- “We take privacy so seriously that we put it under your control.”
 - Only shows you some of the information that they are most obviously capable of connecting to you.
 - Requires that you have an account, be logged in while using services, and maintain a consistent cookie in order to participate.



“If there's something you don't want anyone to know, maybe you shouldn't be doing it in the first place.”

– Eric Schmidt,
Google CEO

“AURORA” WAS ABOUT INTERCEPT

GOOGLESHARING

PREMISE

- The scope of the “Google choice” has become quite large.
- We need some innovation that allows us to reject this type of false choice while still maintaining anonymity.
- We need anonymous access to Google services that is fast and reliable.

GOOGLESHARING

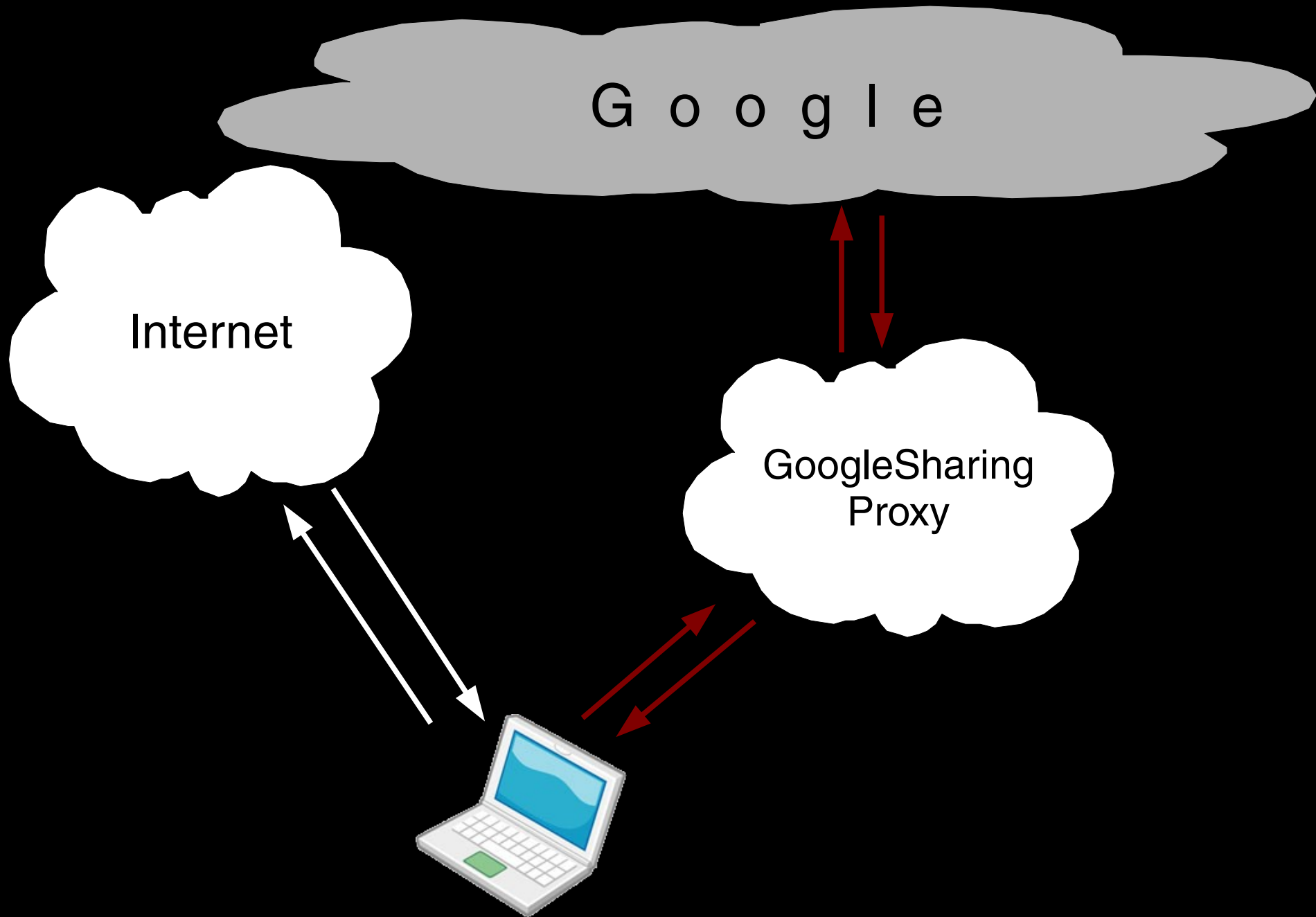


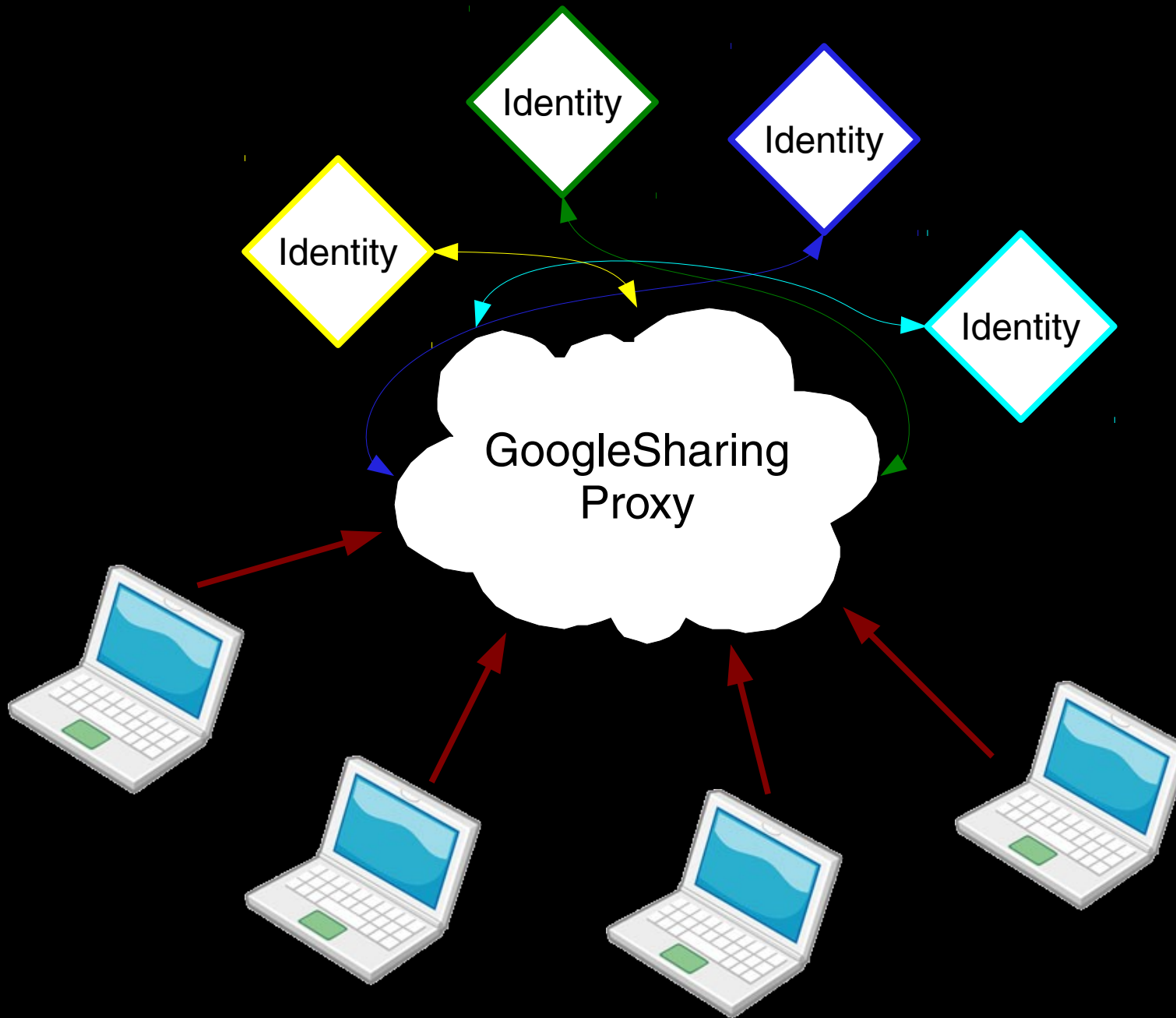
+

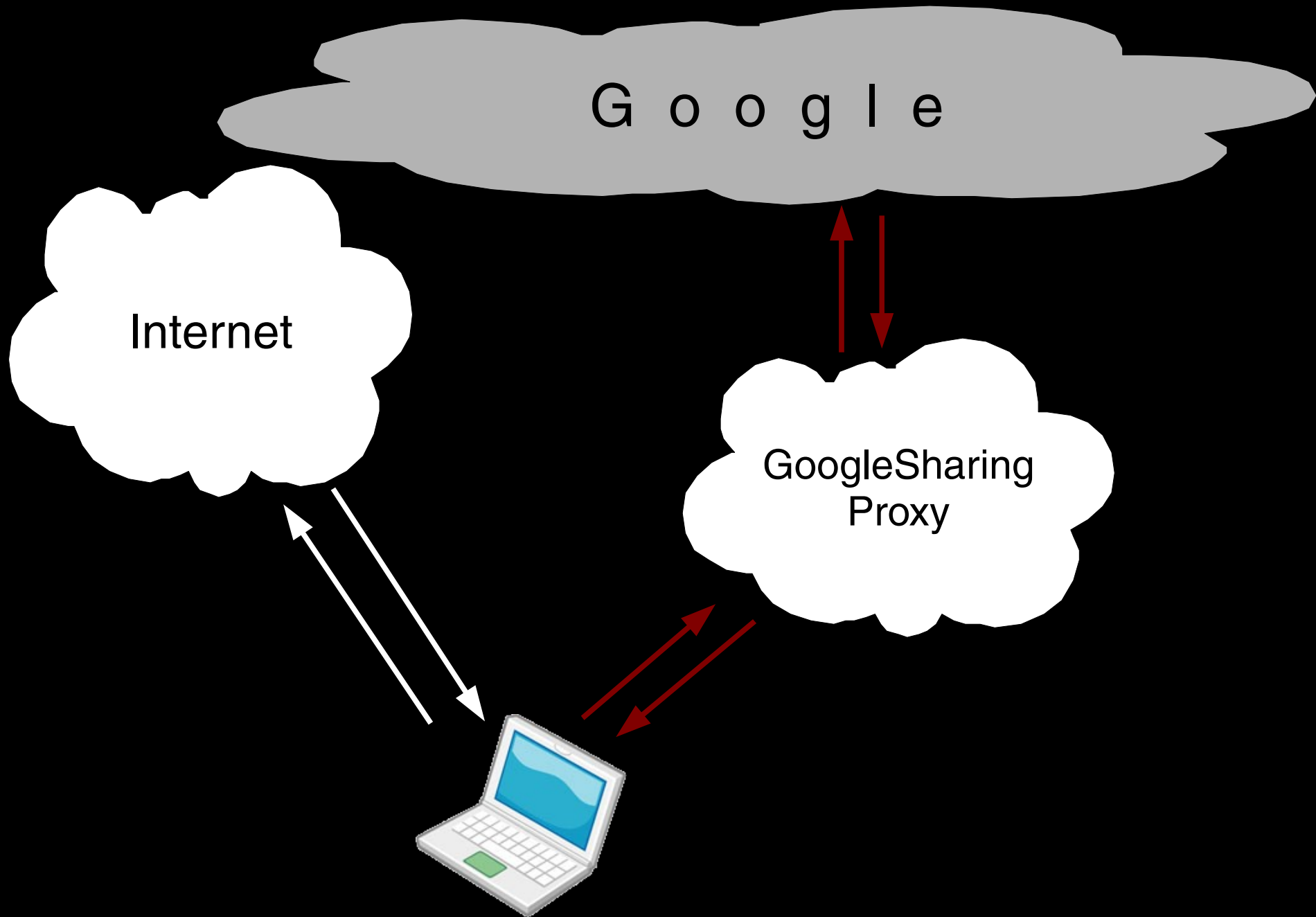


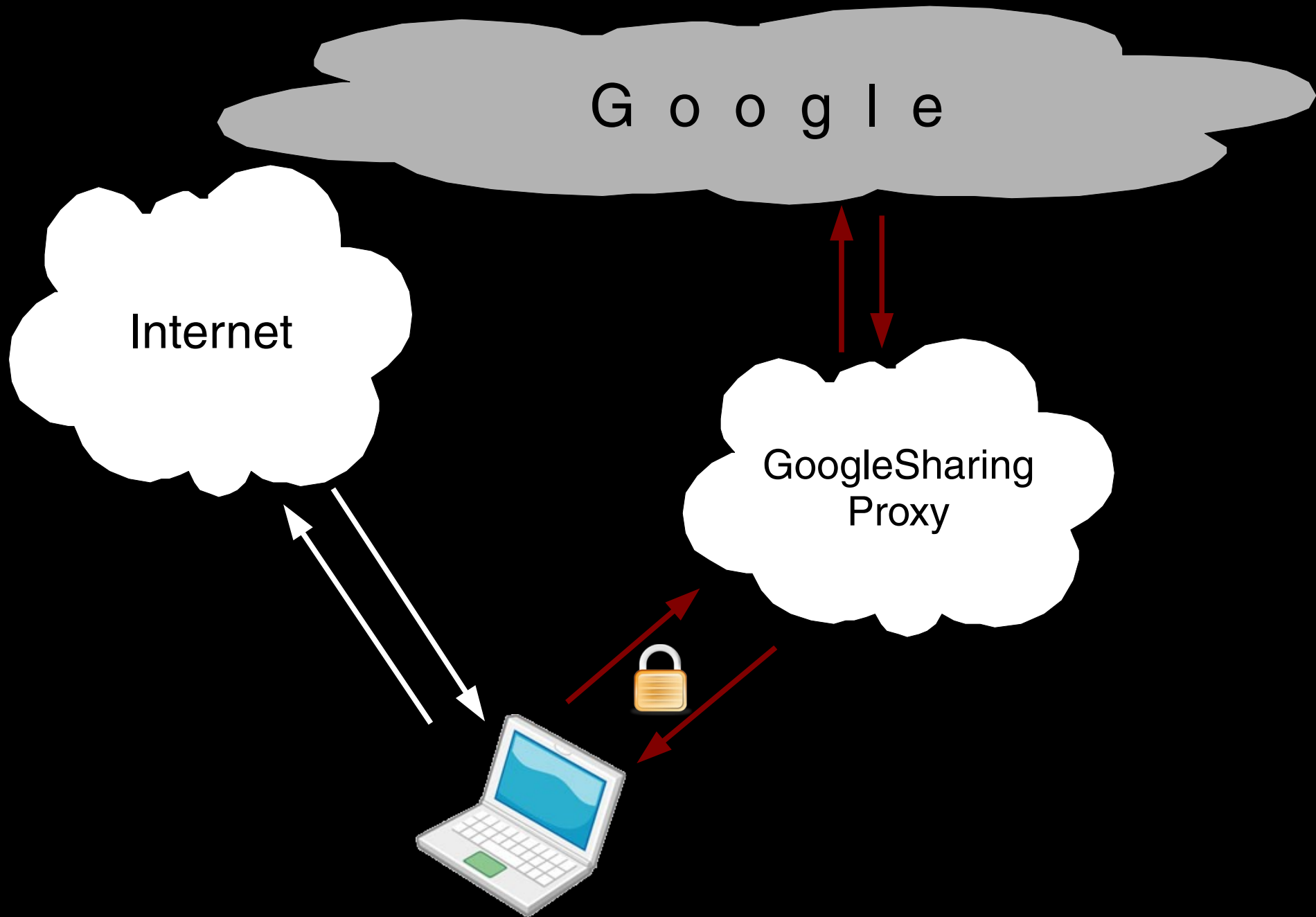
+

GoogleSharing
Proxy Server









pizza, san francisco - Google Maps - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://maps.google.com/

Most Visited Getting Started Latest Headlines

pizza, san francisco - Google M...

Web Images Videos Maps News Shopping Gmail more

New! Help Sign in

Google maps pizza, san francisco

Search Maps Show search options

Find businesses, addresses and places of interest.

Get Directions My Maps

Print Send Link

Traffic More... Map Satellite Terrain

pizza, near San Francisco, CA

Sponsored Links

Escape From NY Pizza - Show on map »
 Order Pizza Online or Call Now.
 Free Pizza Delivery, San Francisco.
 EscapeFromNYPizza.com
 333 Bush Street, San Francisco, CA

North Beach Pizza - more info »

 1462 Grant Avenue, San Francisco, CA - (415) 433-2444
 ★★★★★ 100 reviews
 "Whenever I order a North Beach pizza, I'm always disappointed by the measly ..."

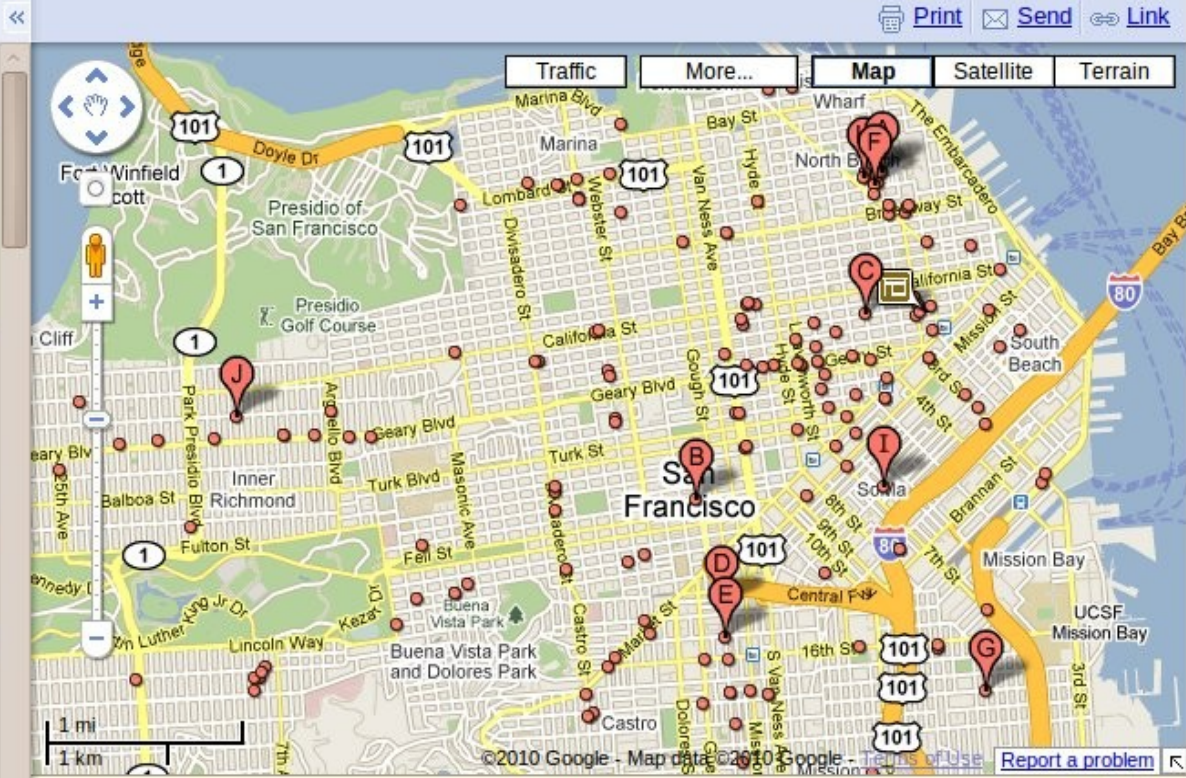
Patxi's Chicago Pizza - more info »

 511 Hayes Street, San Francisco, CA - (415) 558-9991
 ★★★★★ 62 reviews
 "This place has great chicago-style pizza-- something you see too little ..."

Domino's® Pizza - www.Dominos.com - Get 2 Medium 2-Topping Pizzas for \$5.99

Done

Google Sharing Enabled



Business - Google News - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://news.google.com/news/section?pz=1&cf=all&ned=us&topic=b&ict=ln

Most Visited Getting Started Latest Headlines

Business - Google News

Web Images Videos Maps News Shopping Gmail more Sign in

Google news Search News Search the Web Advanced news search Preferences

U.S. Business Updated 5 minutes ago

Top Stories Starred World U.S. Business Sci/Tech Entertainment Sports Health Spotlight Most Popular

All news Headlines Images

Fed gets new oversight powers under Dodd bill: sources
Reuters - Jim Young - 15 minutes ago
Senator Christopher Dodd (D-CT) addresses the AFL-CIO Building and Construction Trades Presidential Candidates Forum in Washington, in this March 28, 2007 file photo.
[Dodd's Financial Overhaul Plan Said to Transform Fed Powers](#) BusinessWeek
[Dodd seeking middle ground on new financial rules](#) The Associated Press
[New York Times](#) - [Politico](#) - [Financial Times](#) - [WBUR](#)
[all 144 news articles »](#) ☐ Email this story

Wen Rebuffing Yuan Calls Risks Retaliation From US Congress
BusinessWeek - 4 hours ago
March 15 (Bloomberg) -- Chinese Premier Wen Jiabao rebuffed calls for the yuan to appreciate, risking a further downturn in relations with the US where lawmakers and economists say his stance is hampering a global recovery.
[Chinese premier slams US 'protectionism,' says yuan is not too low](#) Los Angeles Times
[Wen links inflation to Communist party future](#) Financial Times
[Wall Street Journal](#) - [Economic Times](#) - [Washington Post](#)
[all 2,185 news articles »](#) ☐ GOOG ☐ Email this story

Toyota, US Can't Replicate Prius Acceleration (Correct)
BusinessWeek - Angela Greiling Keane - 58 minutes ago
March 15 (Bloomberg) -- Tests by Toyota Motor Corp. and US regulators on a Prius hybrid whose driver said it accelerated out of control couldn't replicate his account, according to a report prepared for US lawmakers.
[Investigation questions Prius driver's story: report](#) Reuters

Finance Powered by Google Finance

10am 12pm 2pm 4pm +0.43% +0.21% 0.00% -0.21% -0.43%

Dow 10,624.69 +12.85 (0.12%)
S&P 500 1,149.99 -0.25 (-0.02%)
Nasdaq 2,367.66 -0.80 (-0.03%)

Quotes
Get quotes
Example: "CSCO" or "Google"

In the news
GOOG 579.54 -1.60 (-0.28%)
TM 76.99 +0.05 (0.06%)
TOM 28.19 -0.10 (-0.37%)

Google Sharing Enabled

Done

FACECLOAK

PROF. URS HENGARTNER



Name:

Matches:

Email

→

Add as Friend

Send a Message

View Friends



Name:

Matches:

Email

→

Email Your Keys

Send a Message

View Friends

Full Name:

Wanying Luo

Your Email:

w8luo@uwaterloo.ca

New Password:

••••••

I am:

Male

▼

Birthda:

▼

▼

▼

Why do I need to provide this?

Full Name:

@@John Doe

Your Email:

w8luo@uwaterloo.ca

New Password:

••••••

I am:

Male

▼

Birthda:

@@Jul

@@8

@@1988

▼

Why do I need to provide this?

TWITTER BROADCAST || CONVERSATION

SECOND THESIS

CRYPTO WAR → DATA FREEDOM

FUTURE OF DATA CONTROL

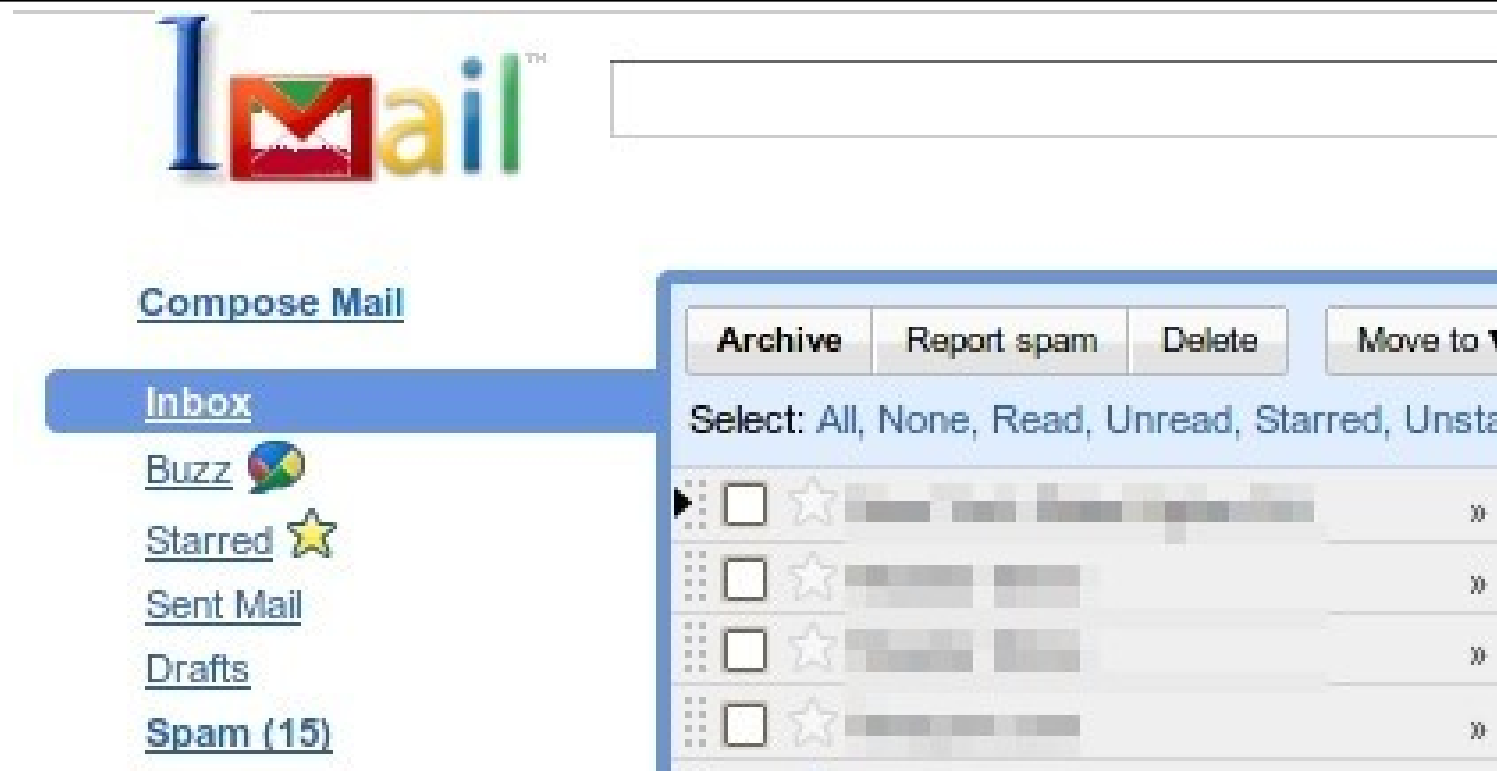
PROJECTS BORN OUT OF REALITY

DARKNETS, DATA HAVENS, HIDDEN SERVICES

NOT THE FUTURE WE GOT

PRIVACY ADVOCATES LOVE “THE OTHER.”

“IRAN LAUNCHES NATIONAL EMAIL SERVICE”



LOSS ON CRYPTO
GIVING UP → CHANGING STRATEGIES

KEY ESCROW → KEY DISCLOSURE

REGULATION OF INVESTIGATORY POWERS ACT (RIPA)

KEY DISCLOSURE

NO FORWARD SECURITY

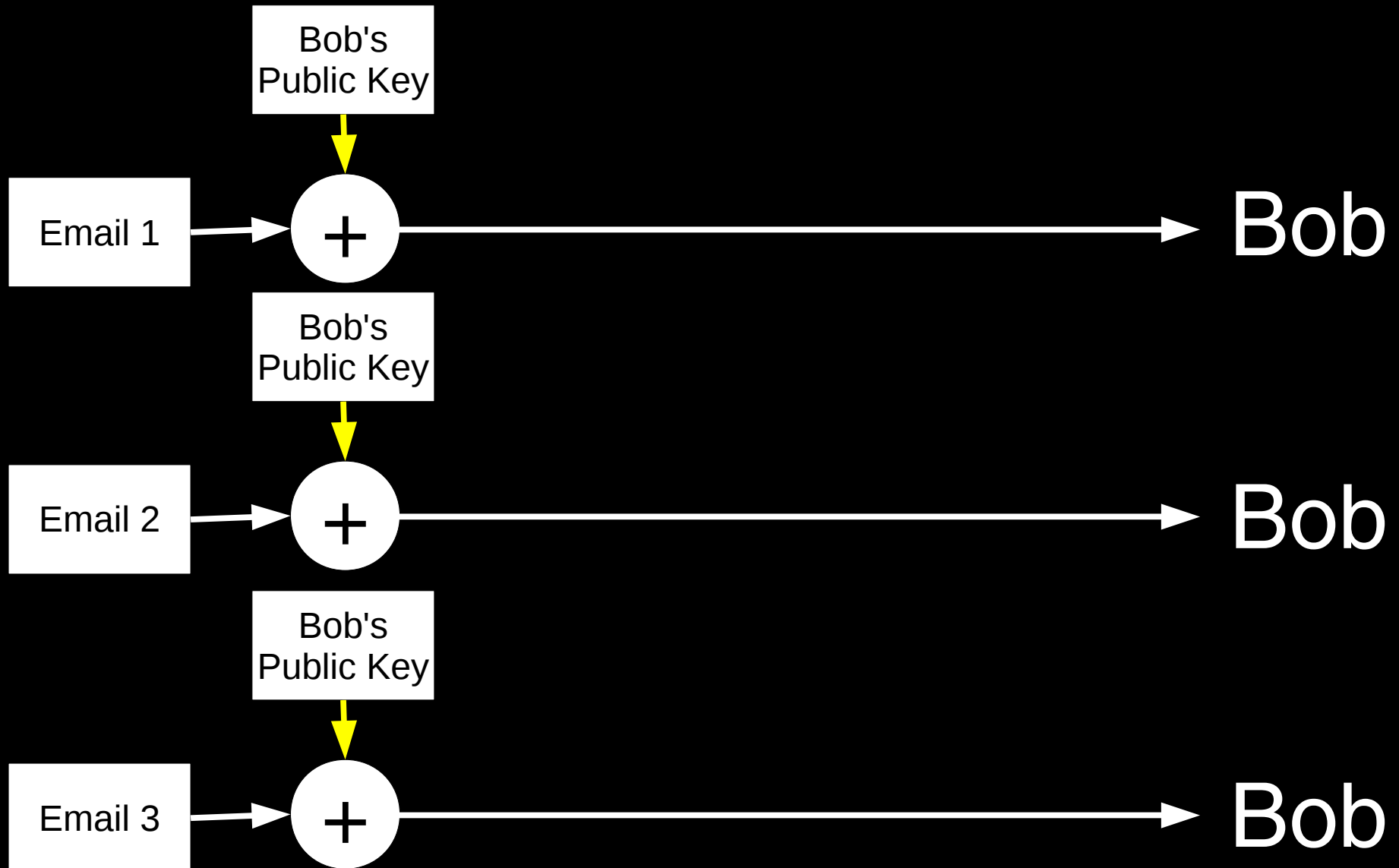
TASKS FOR THE FUTURE

1. Deal with the choices that aren't choices.
2. Worry a little less about information freedom.
3. Worry a lot more about forward security.

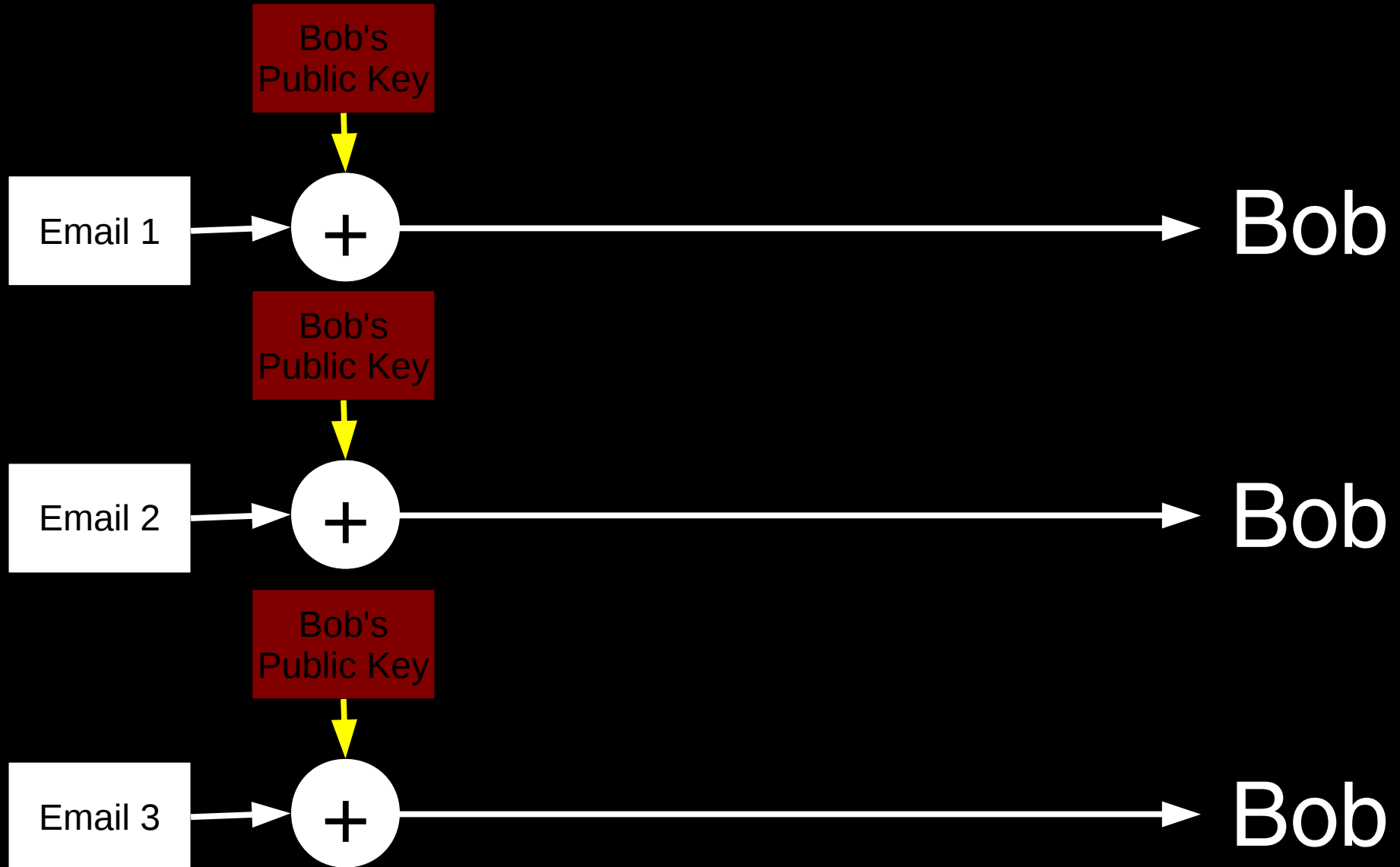
“OFF-THE-RECORD COMMUNICATION,
OR, WHY NOT TO USE PGP”

- NIKITA BORISOV, IAN GOLDBERG, ERIC BREWER

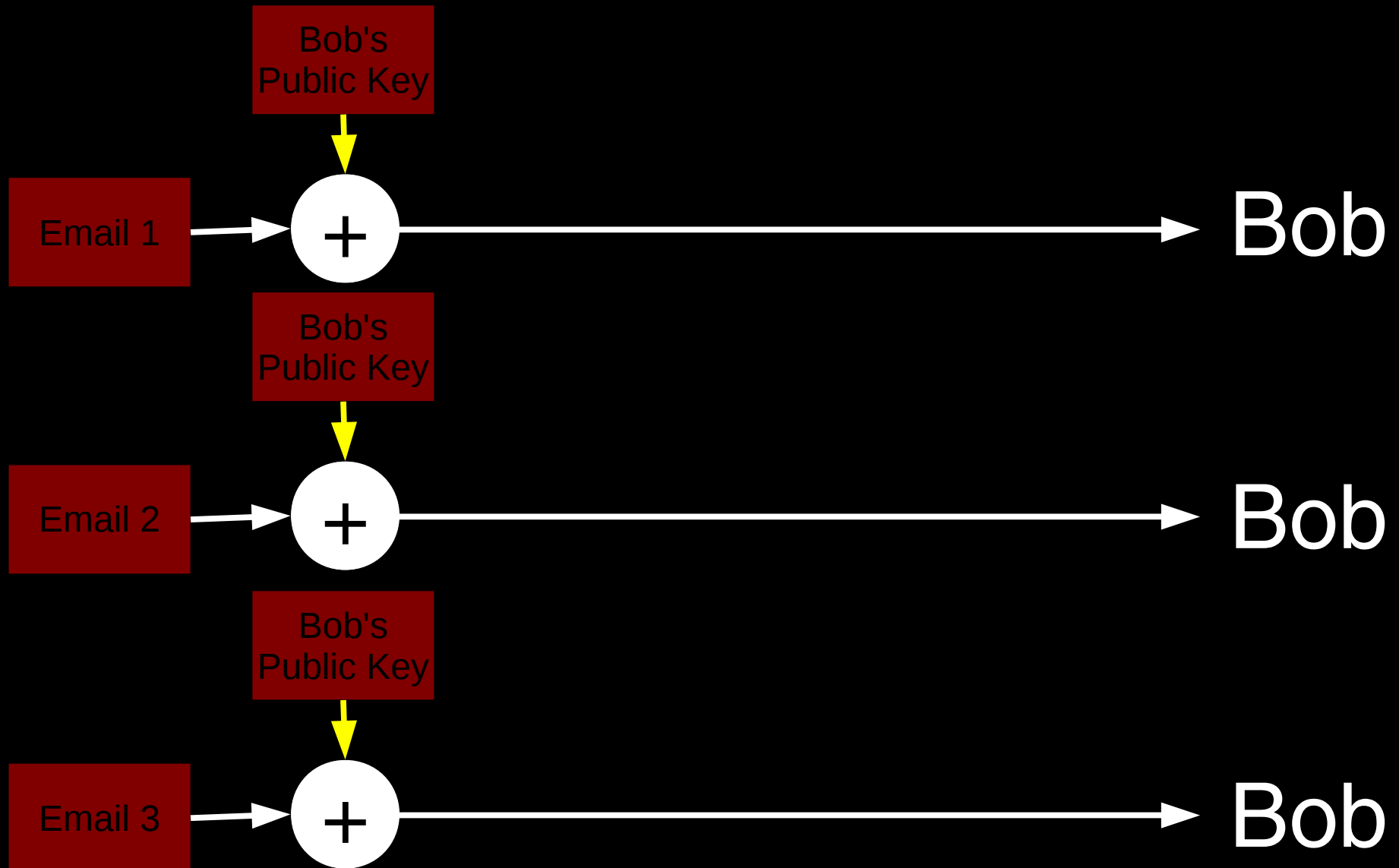
PGP MODEL



PGP MODEL



PGP MODEL



PGP MODEL

- One key compromise affects all previous correspondence.

PGP MODEL

- One key compromise affects all previous correspondence.
- The secrecy of what / write is function of *your* security practices.

PGP MODEL

- One key compromise affects all previous correspondence.
- The secrecy of what / write is function of *your* security practices.
- There is authenticity, but no deniability.

PGP MODEL

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hey Bob, today I was thinking that Eve is a real jerk.

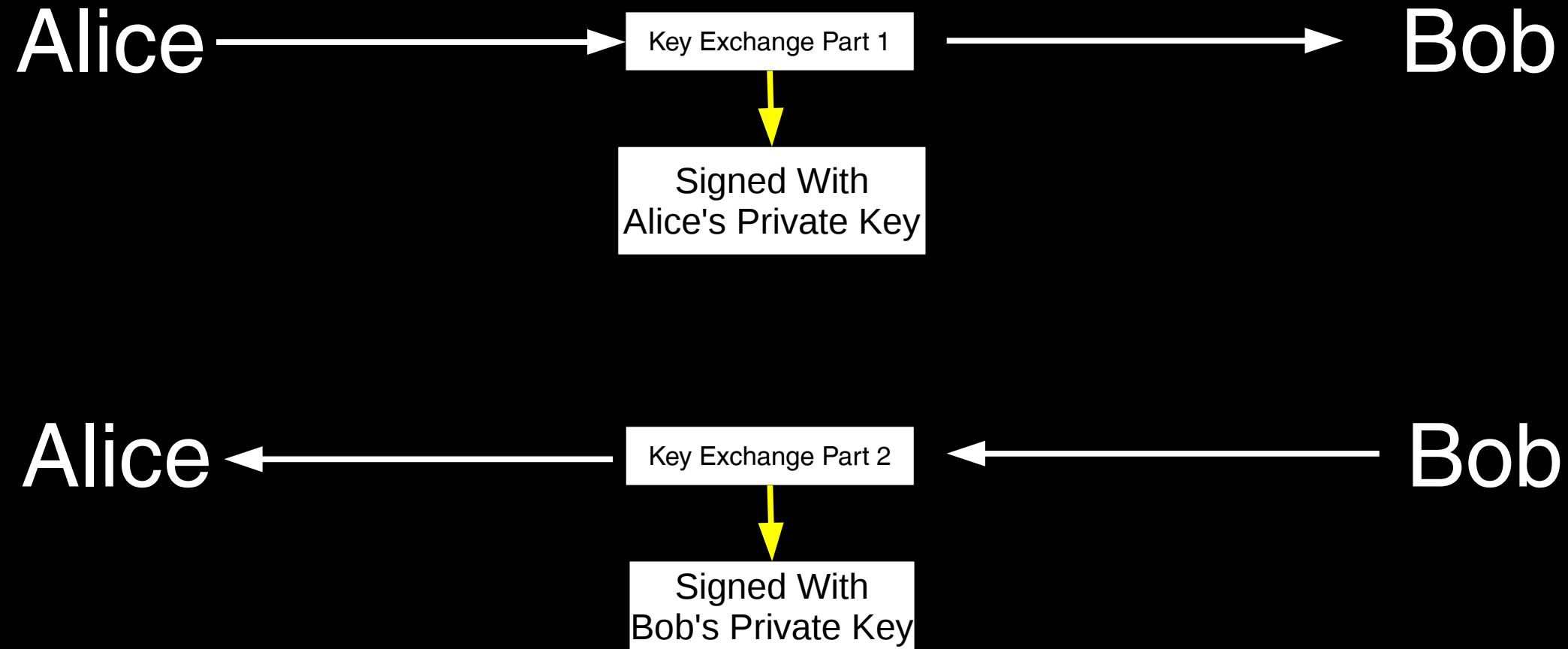
-----BEGIN PGP SIGNATURE-----

iEYEARECAAYFAkumY0MACgkQ2yS3tG03iIJhAACgiufmacfyU
M/9PYcVS2Mdb9tdmhYAoO4P0pZug2D7BuFEPkLovKpipore=8
rKh

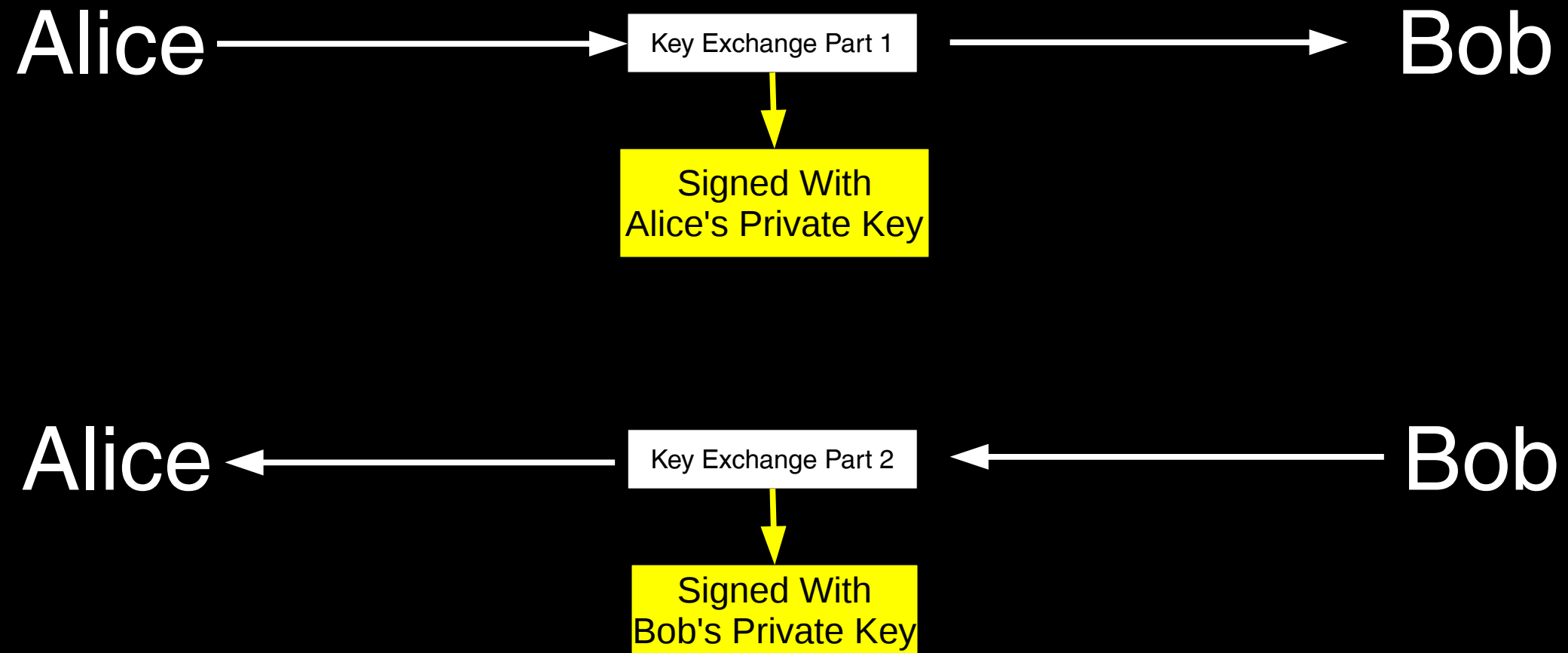
-----END PGP SIGNATURE-----

UNDENIABLE

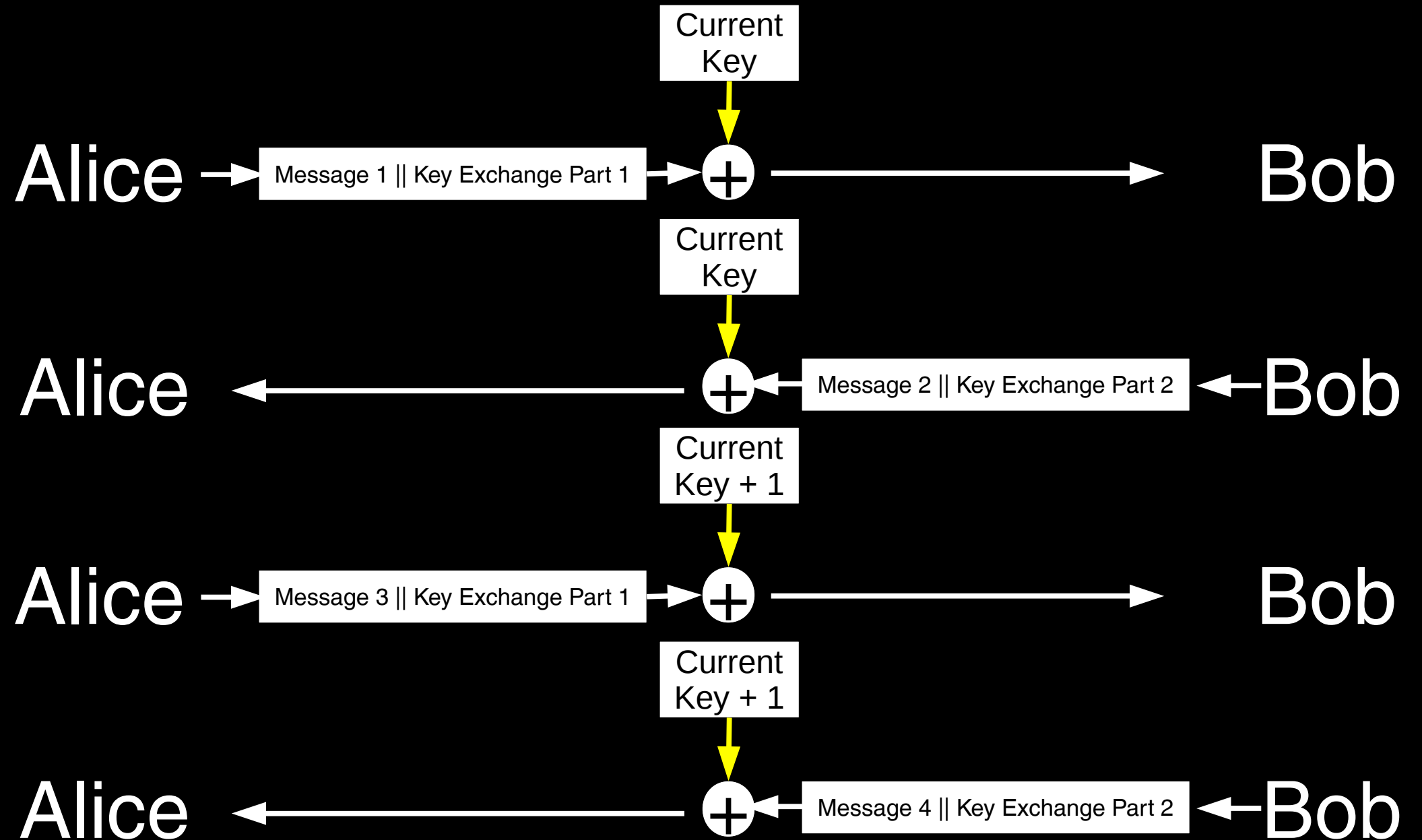
OTR Model



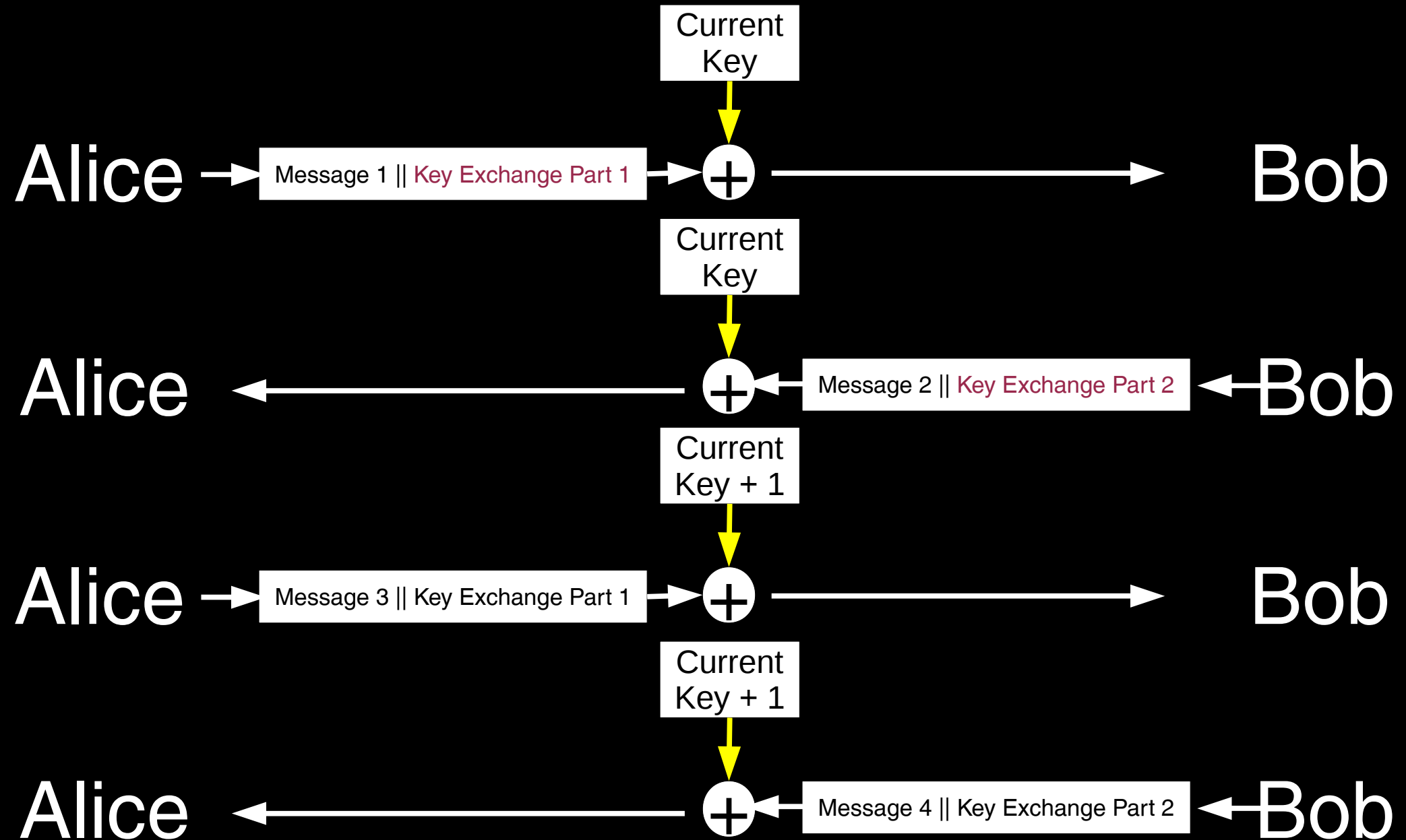
OTR Model



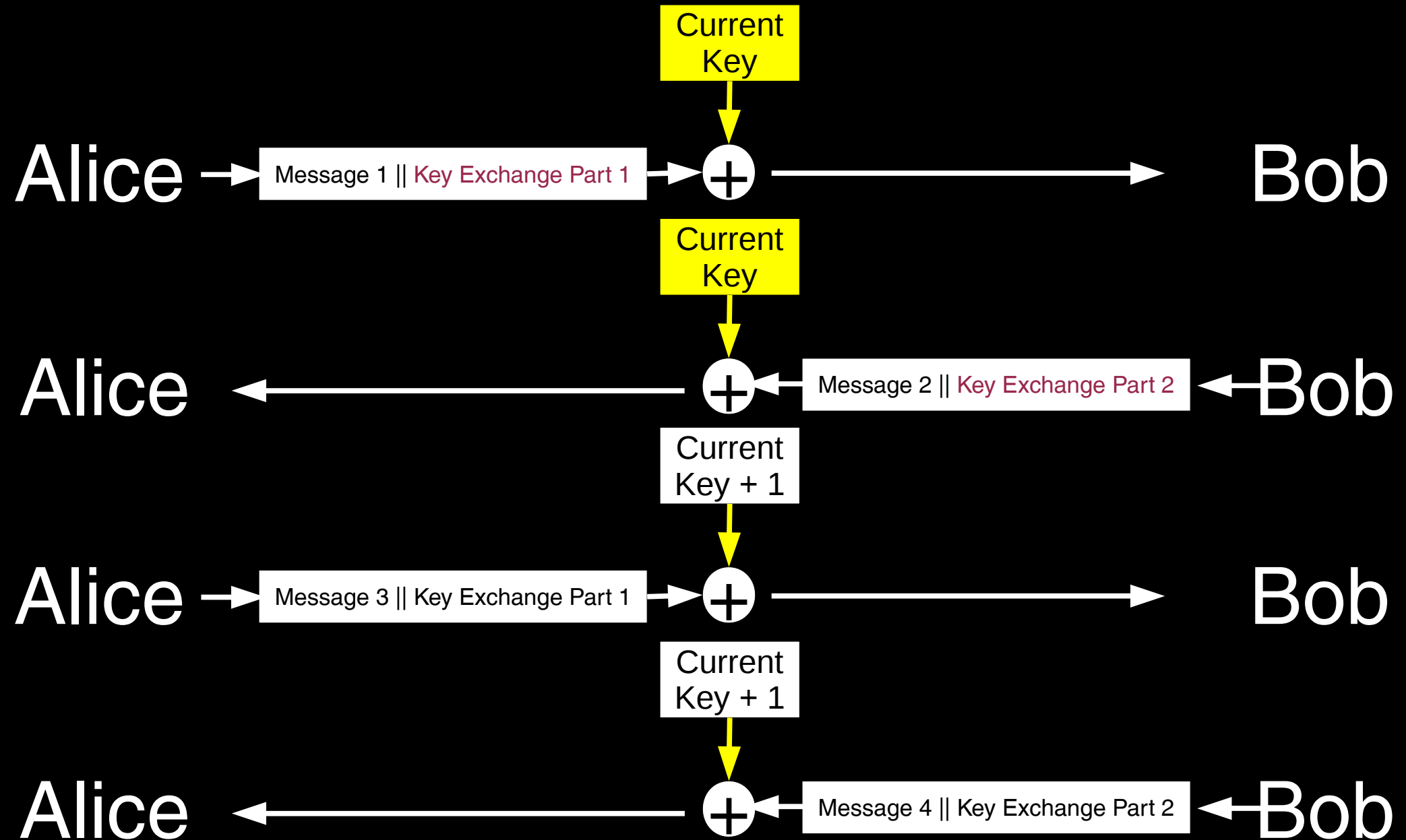
OTR Model



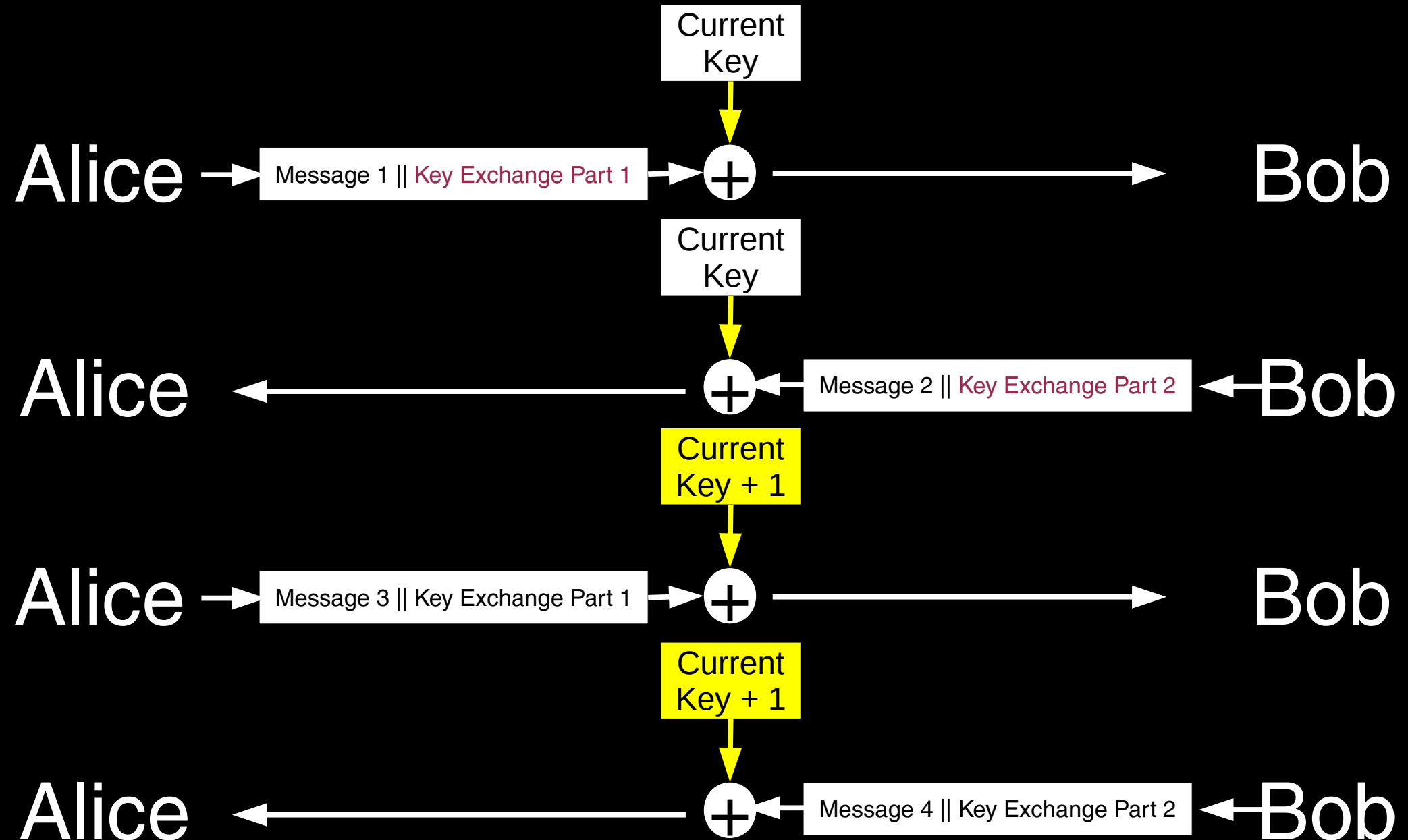
OTR Model



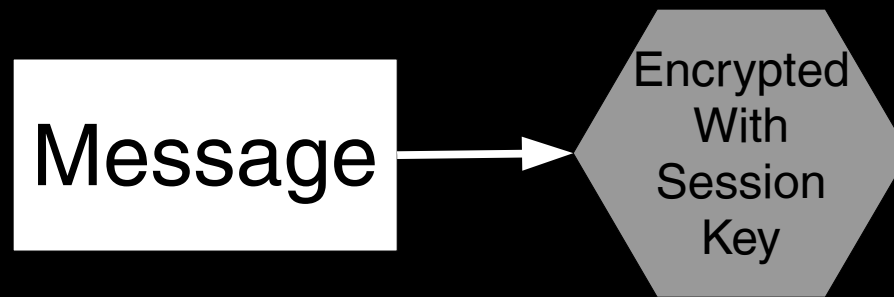
OTR Model



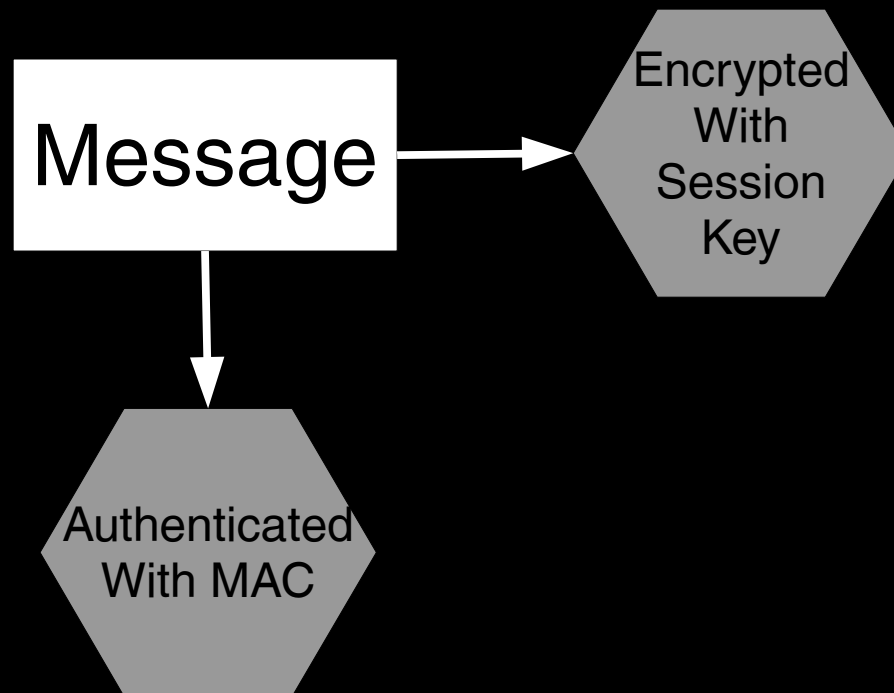
OTR Model



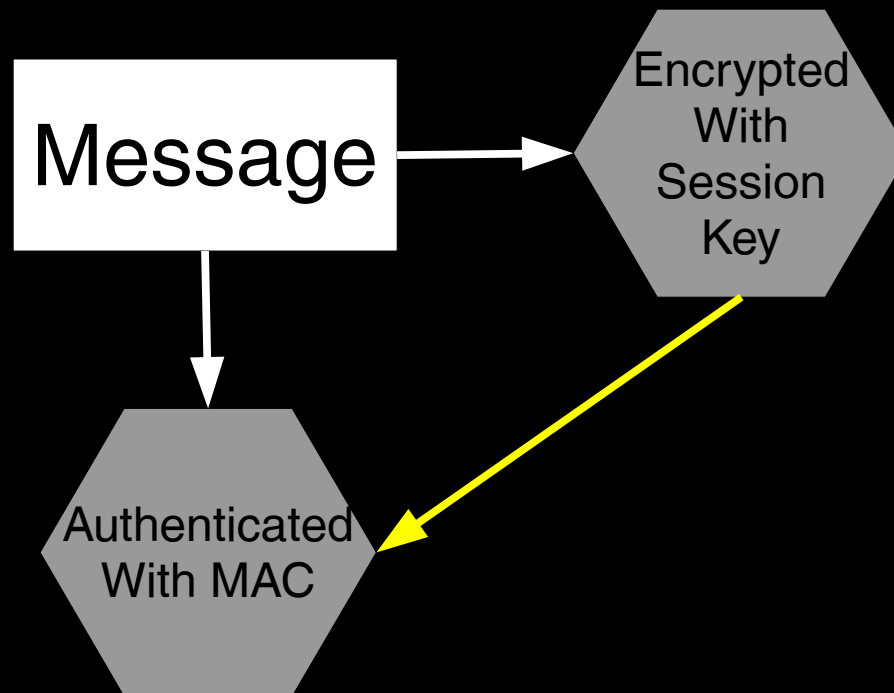
OTR Model



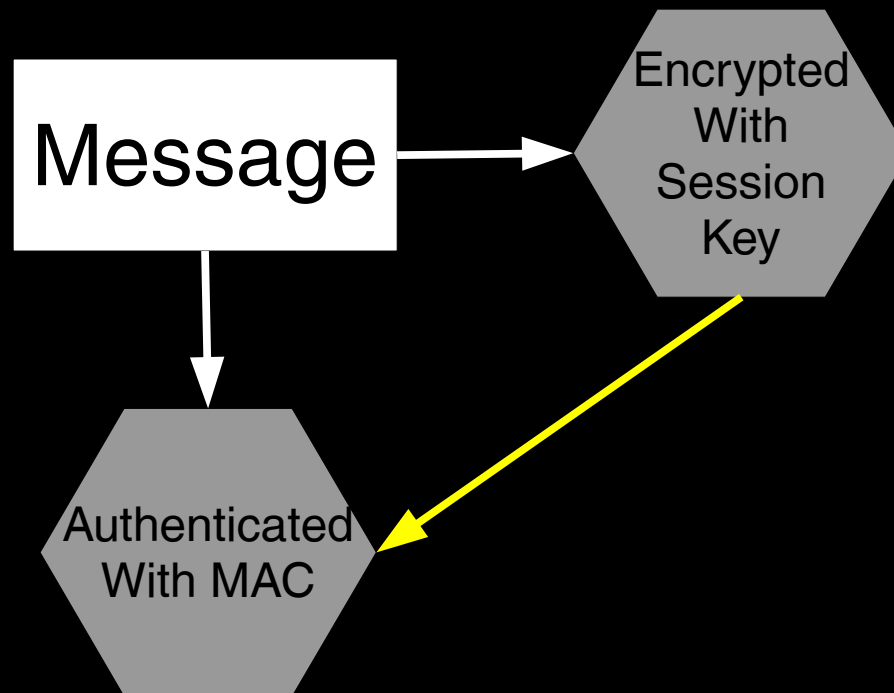
OTR Model



OTR Model

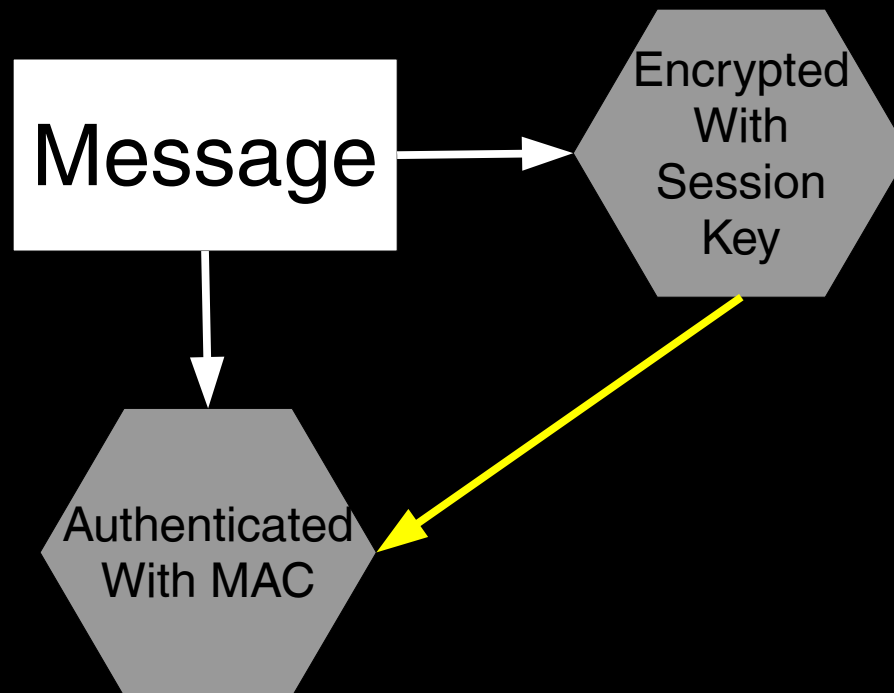


OTR Model



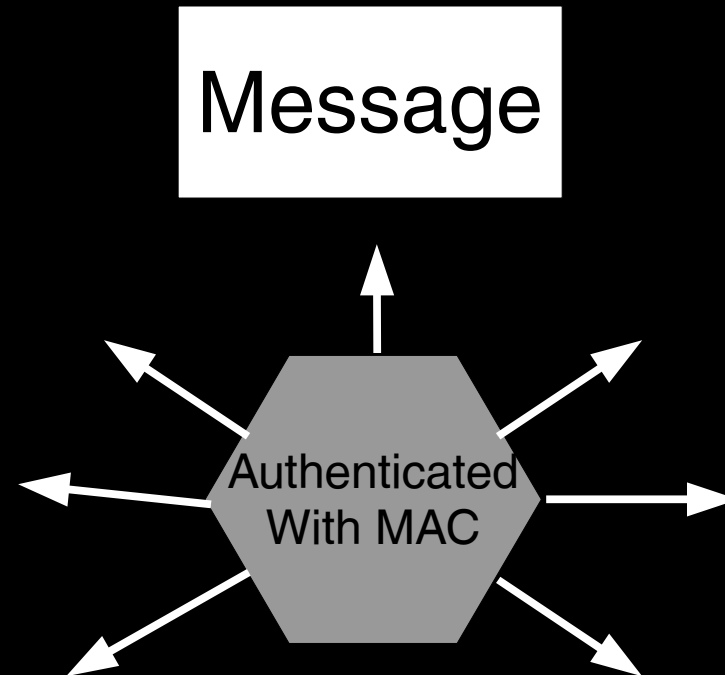
Signatures are undeniable because they have only one possible author.

OTR Model



MACs have *two* possible authors.

OTR Model



After a broadcast, *anyone* can forge an old message.

OTR MODEL

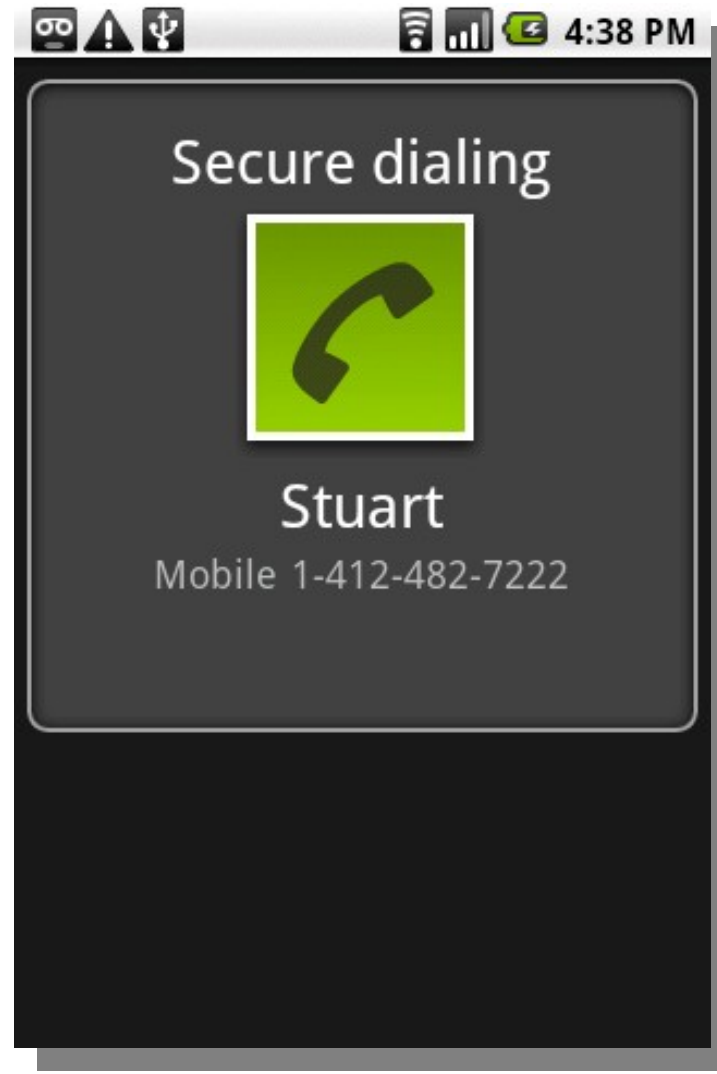
- A key compromise does not affect previous messages.
- You get authenticity, but also deniability.

FUTURE

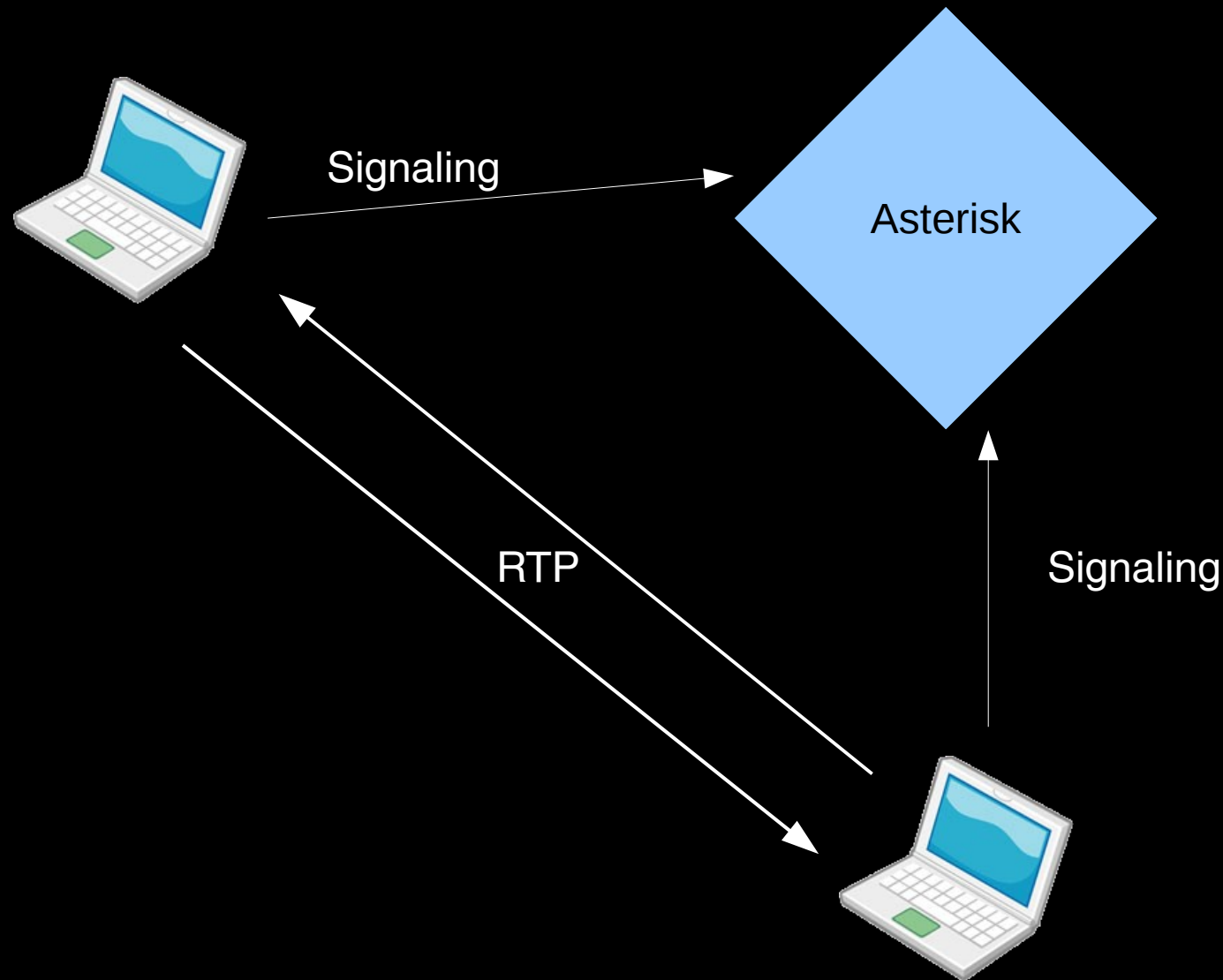
WHISPER SYSTEMS

BRING FORWARD SECURE PROTOCOLS INTO MOBILE PHONES

WHISPER SYSTEMS

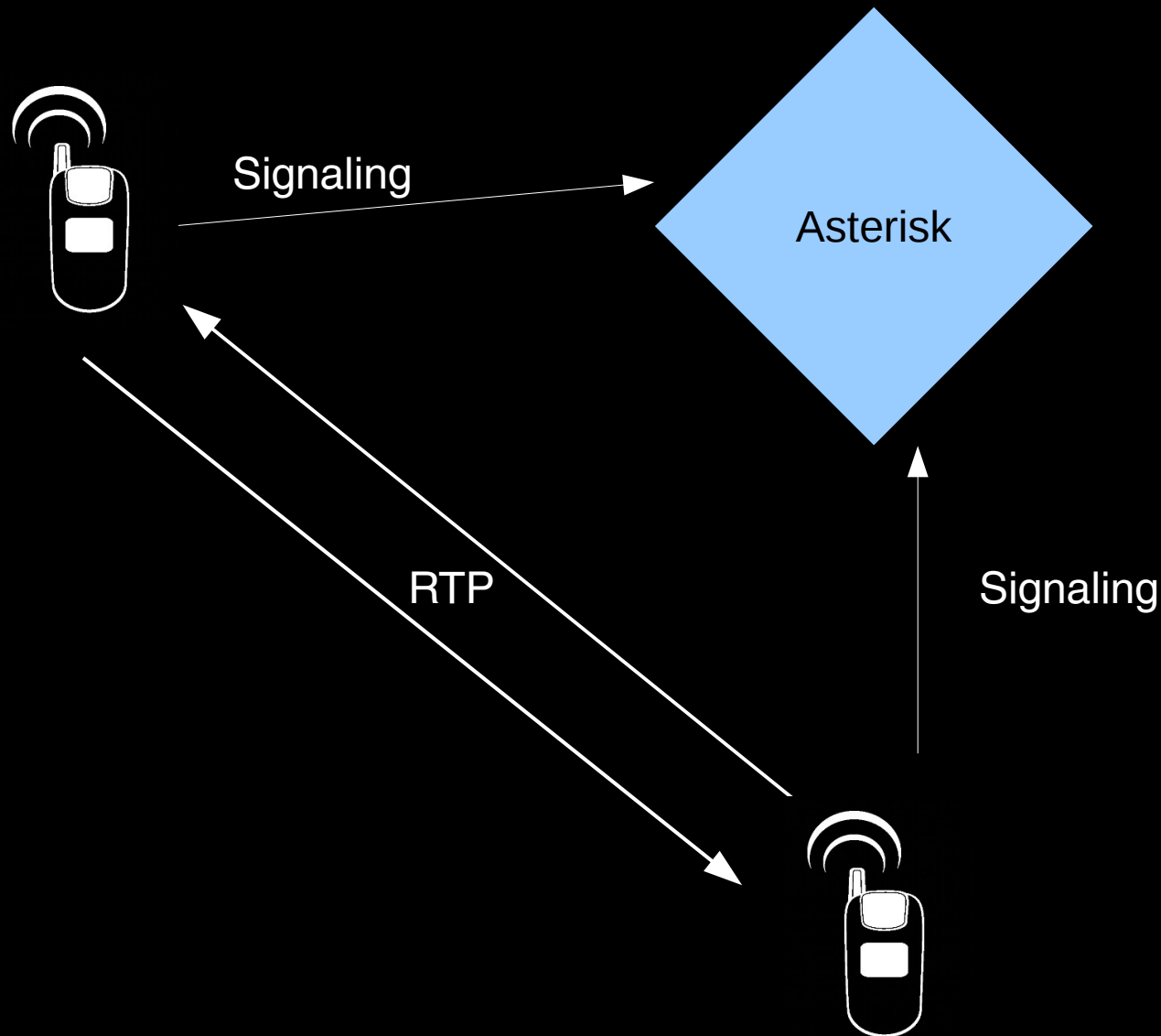


WHISPER SYSTEMS BUT DOESN'T VOIP SUCK?



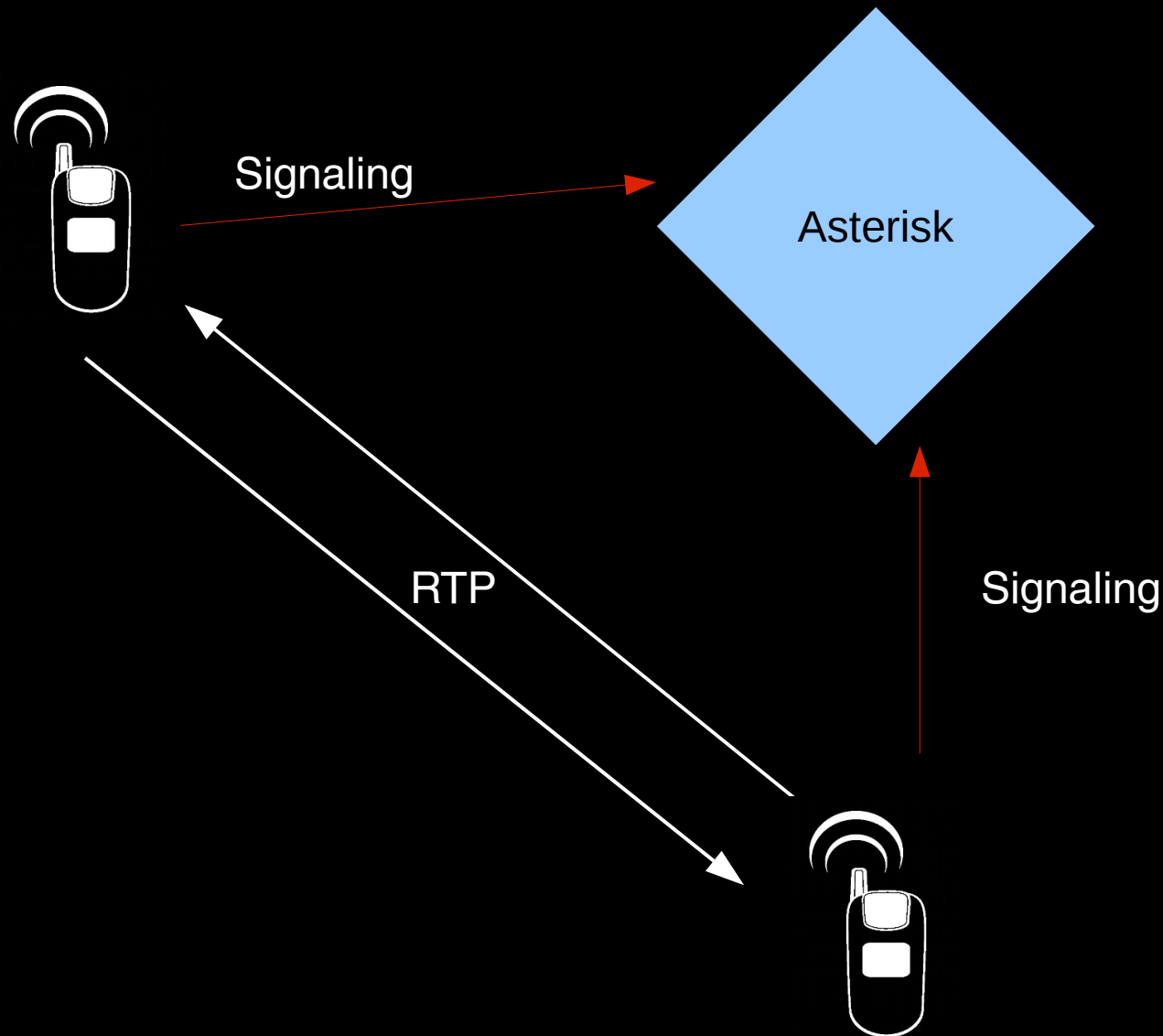
WHISPER SYSTEMS

BUT DOESN'T *mobile* VOIP SUCK?



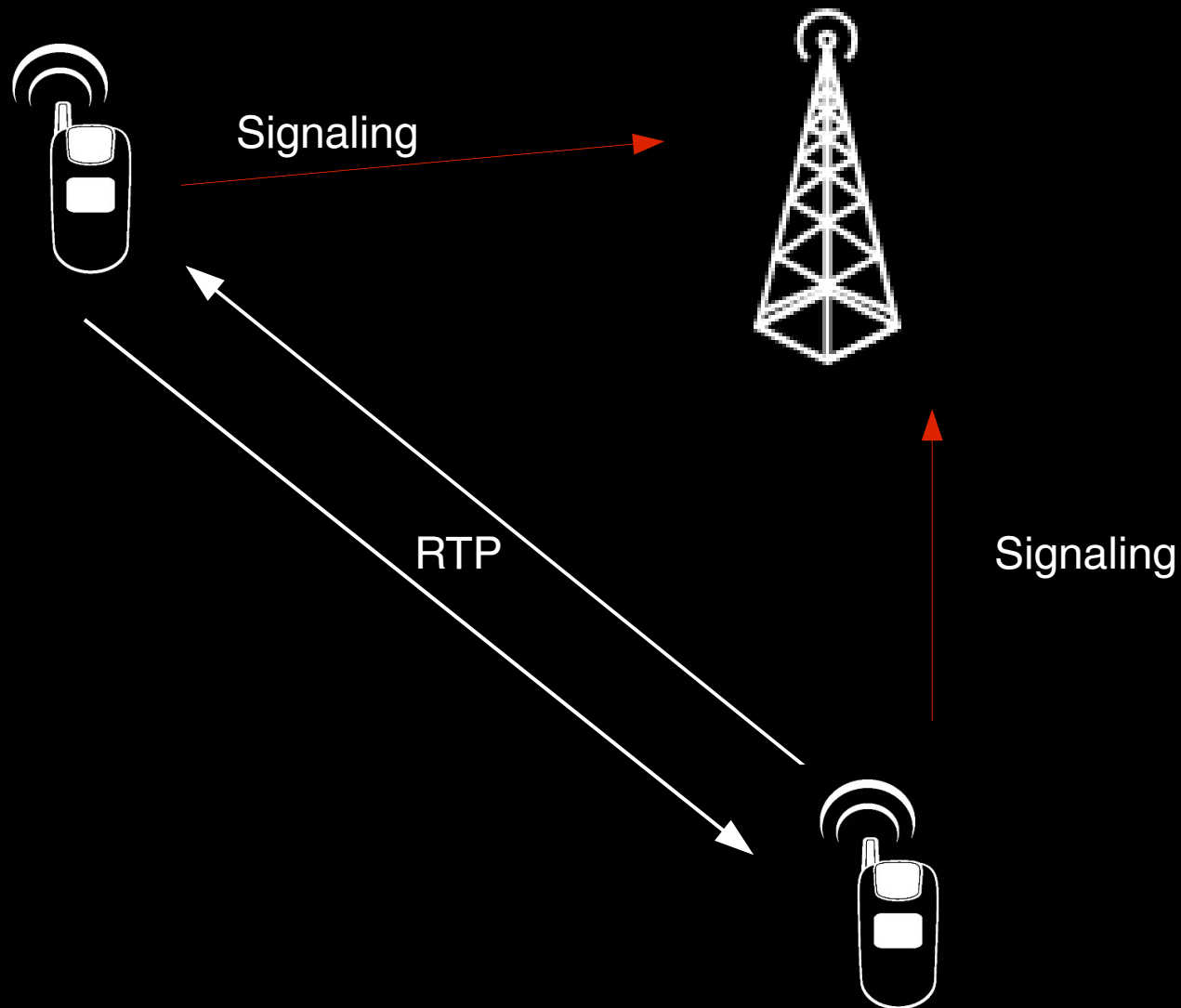
WHISPER SYSTEMS

BUT DOESN'T *mobile* VOIP SUCK?



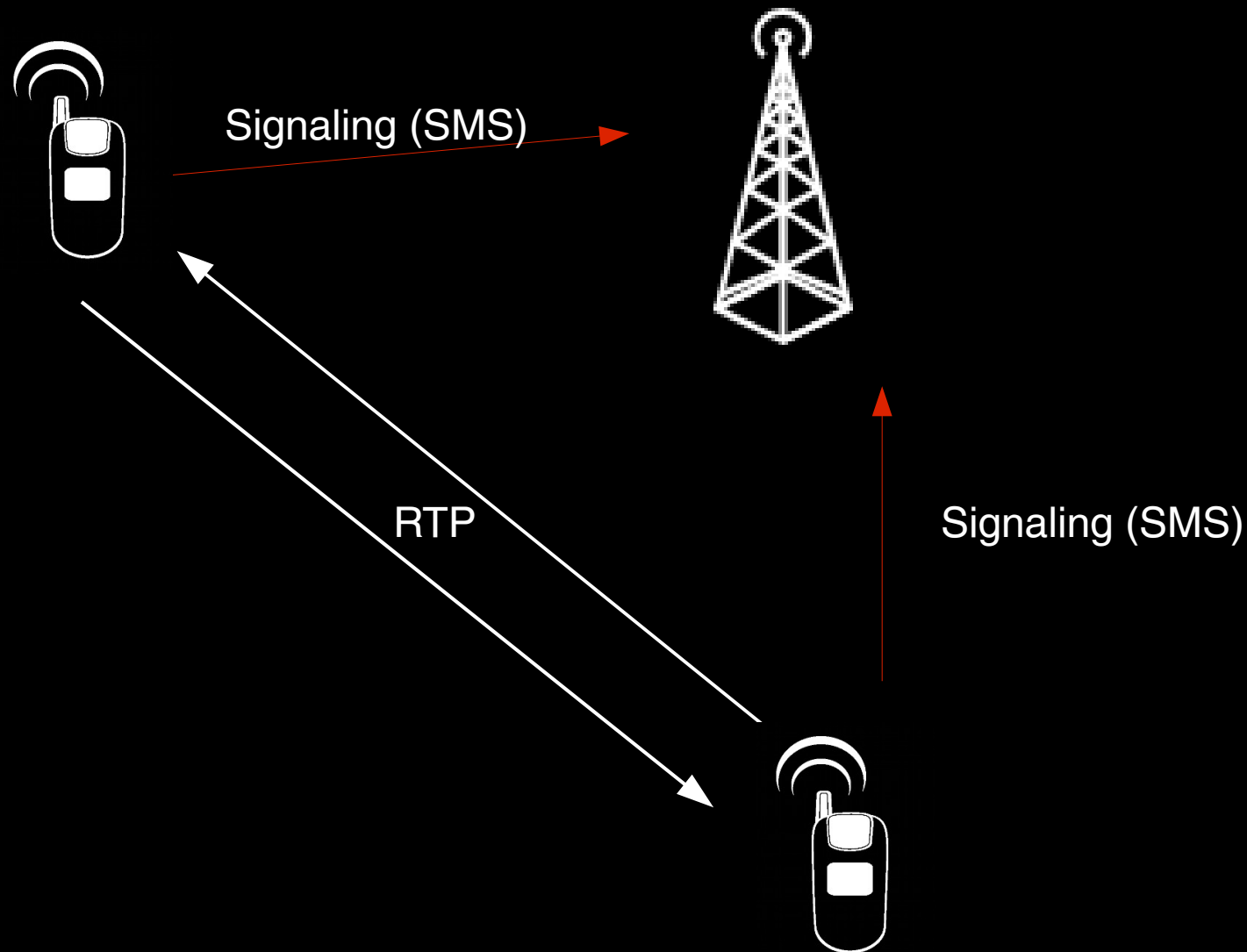
WHISPER SYSTEMS

BUT DOESN'T *mobile* VOIP SUCK?



WHISPER SYSTEMS

BUT DOESN'T *mobile* VOIP SUCK?

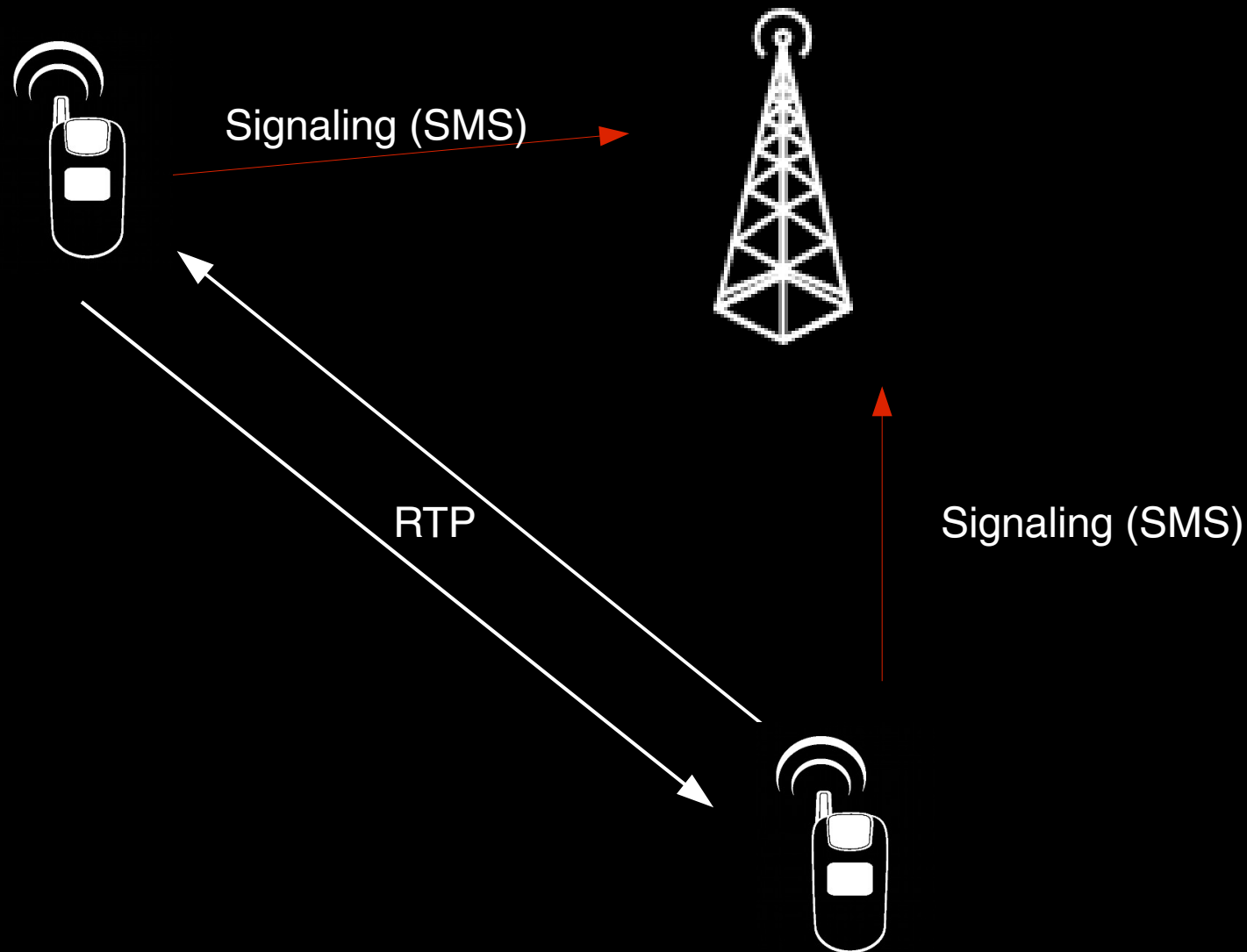


WHISPER SYSTEMS

- Your phone doesn't need to maintain a constant network connection to a SIP server.
 - (Your phone can go to sleep!)
- You don't need the equivalent of a Skype ID.
 - (Addressing is based on existing phone numbers!)
- You don't need to run a VOIP server.
 - (Just install the app and you're ready!)

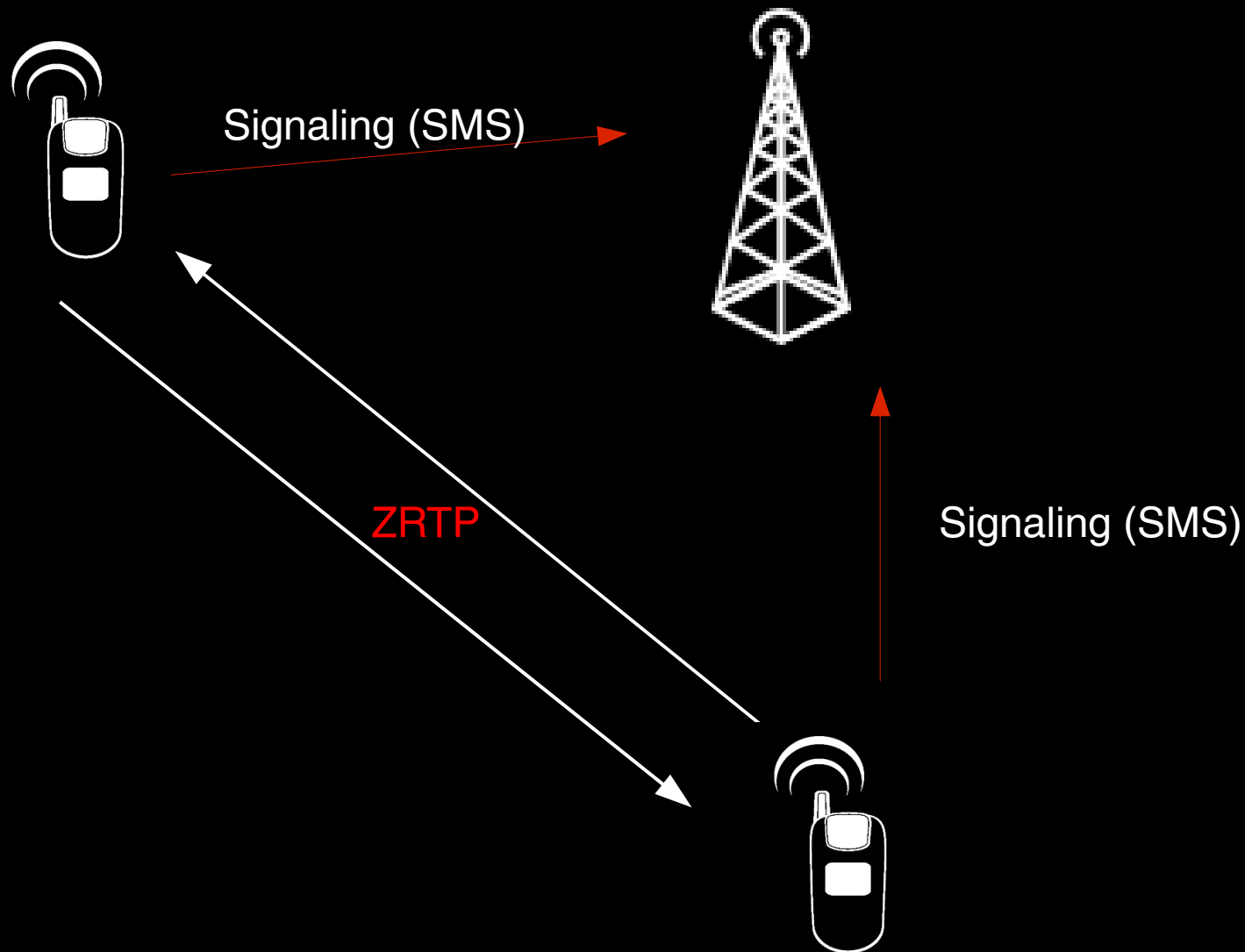
WHISPER SYSTEMS

BUT DOESN'T *mobile* VOIP SUCK?



WHISPER SYSTEMS

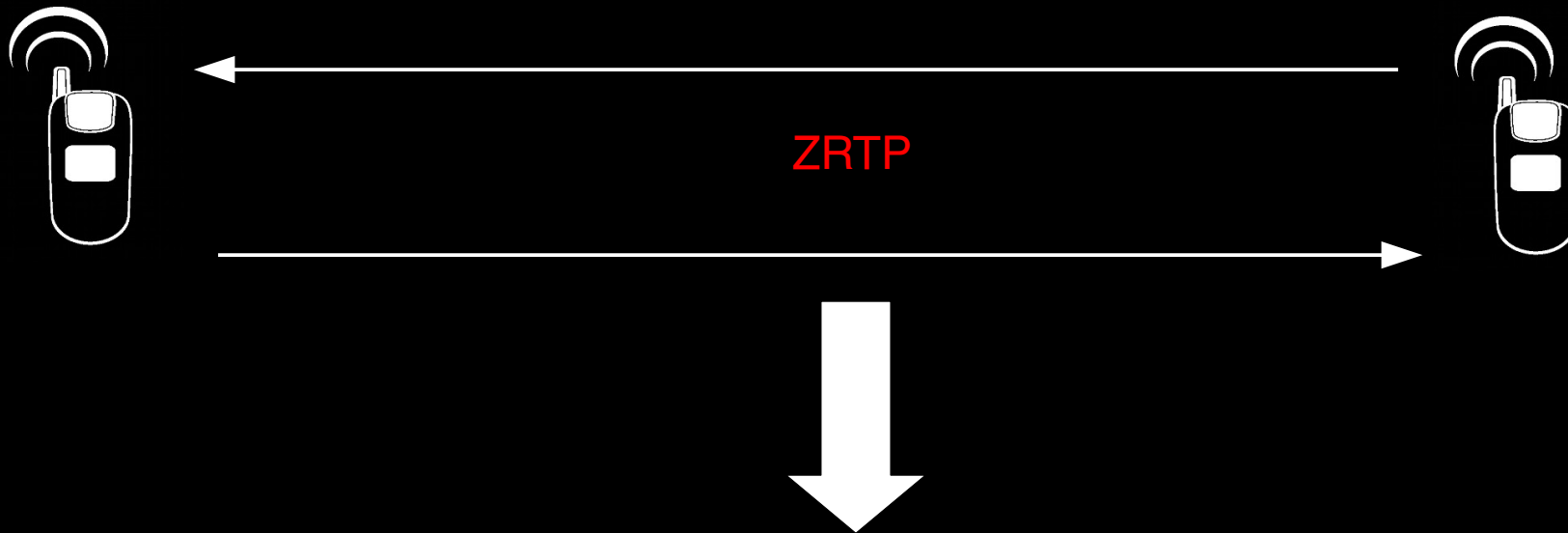
BUT DOESN'T *mobile* VOIP SUCK?



ZRTP



ZRTP



Negotiate ephemeral session key.

ZRTP

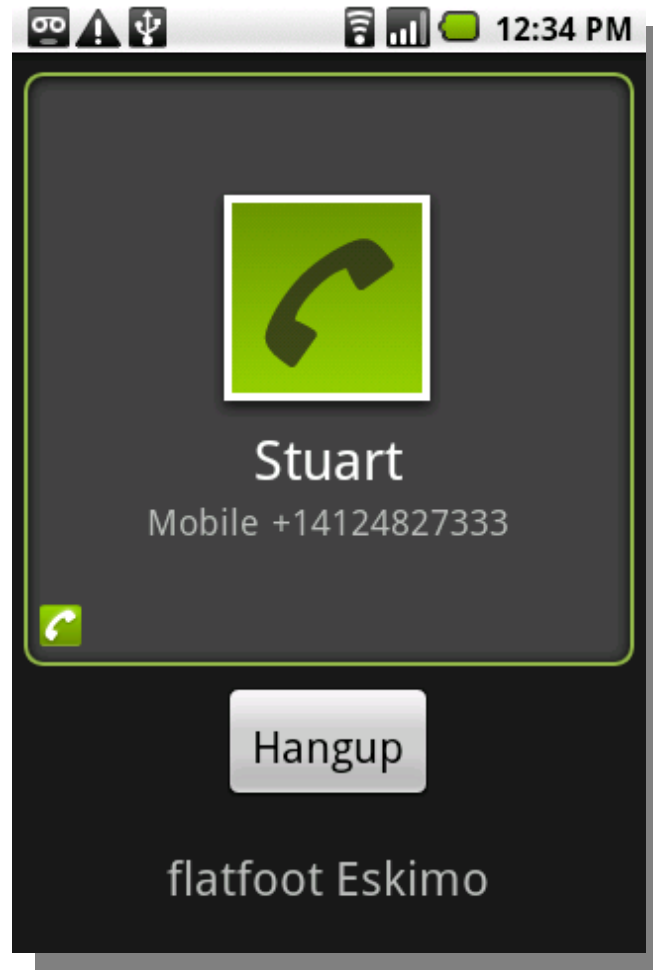


Negotiate ephemeral session key.



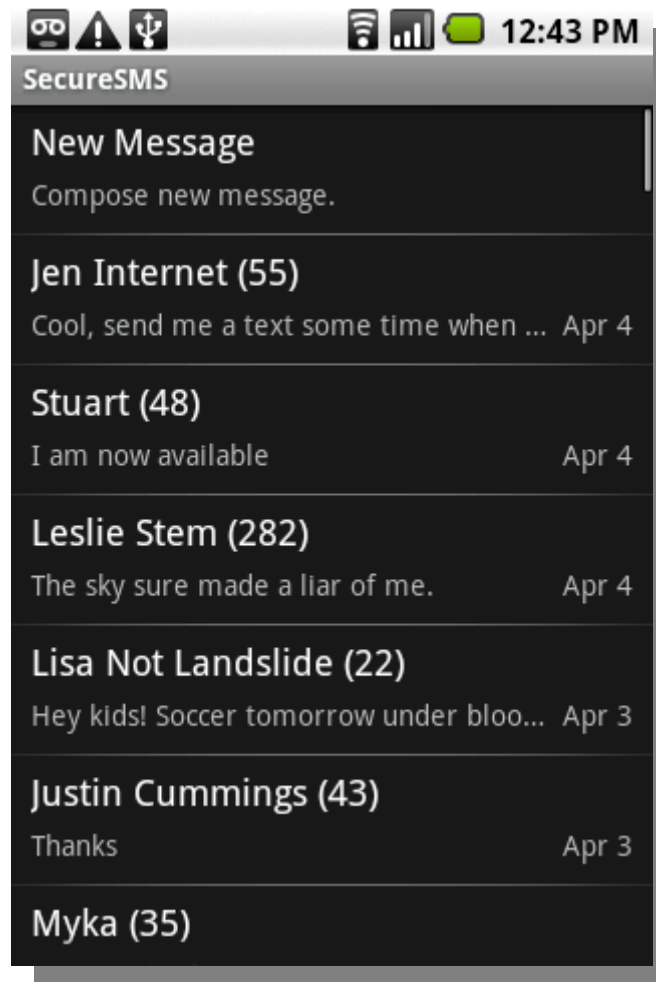
Derive “Short Authentication String”.

ZRTP

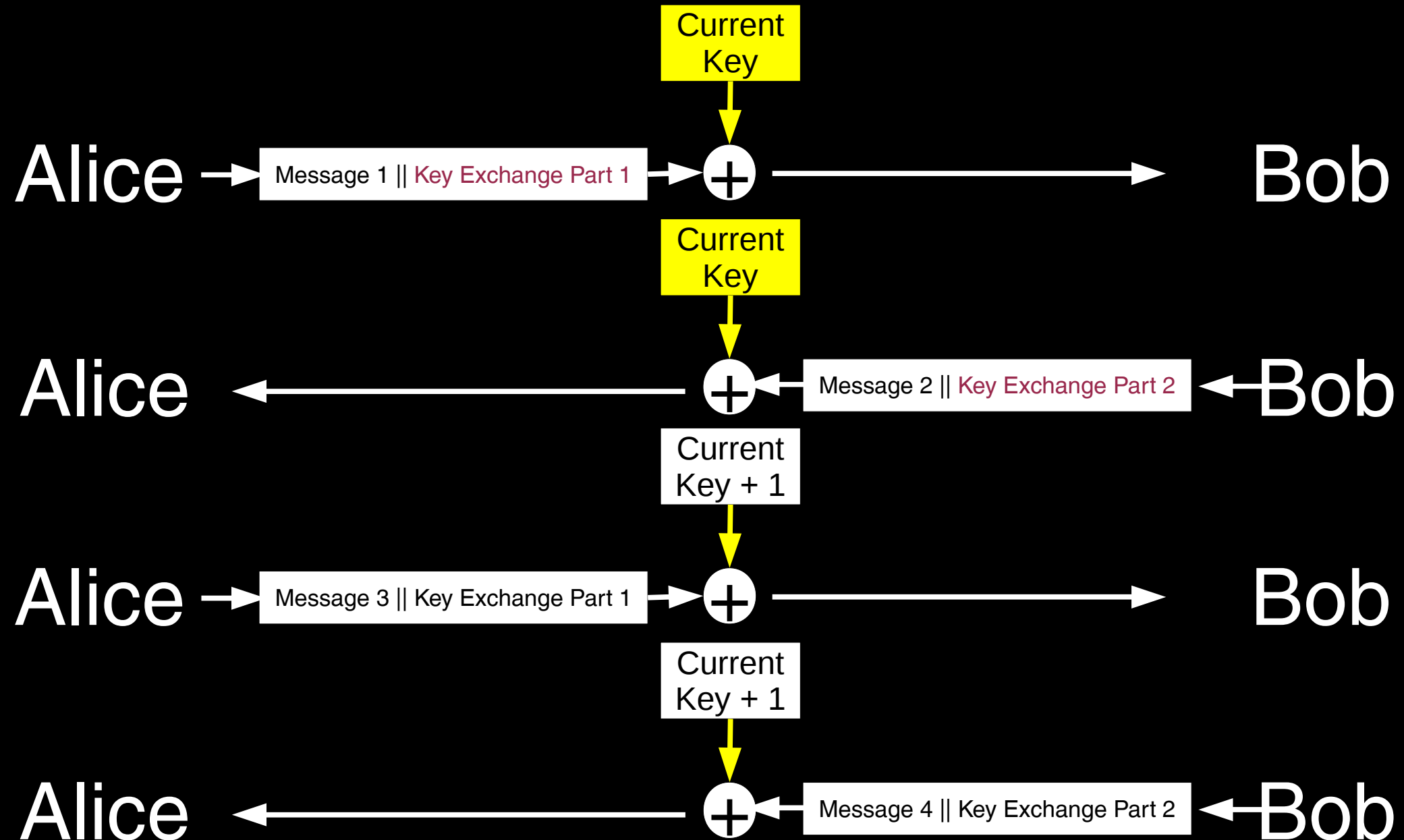


WHISPER SYSTEMS OTR-DERIVED SMS

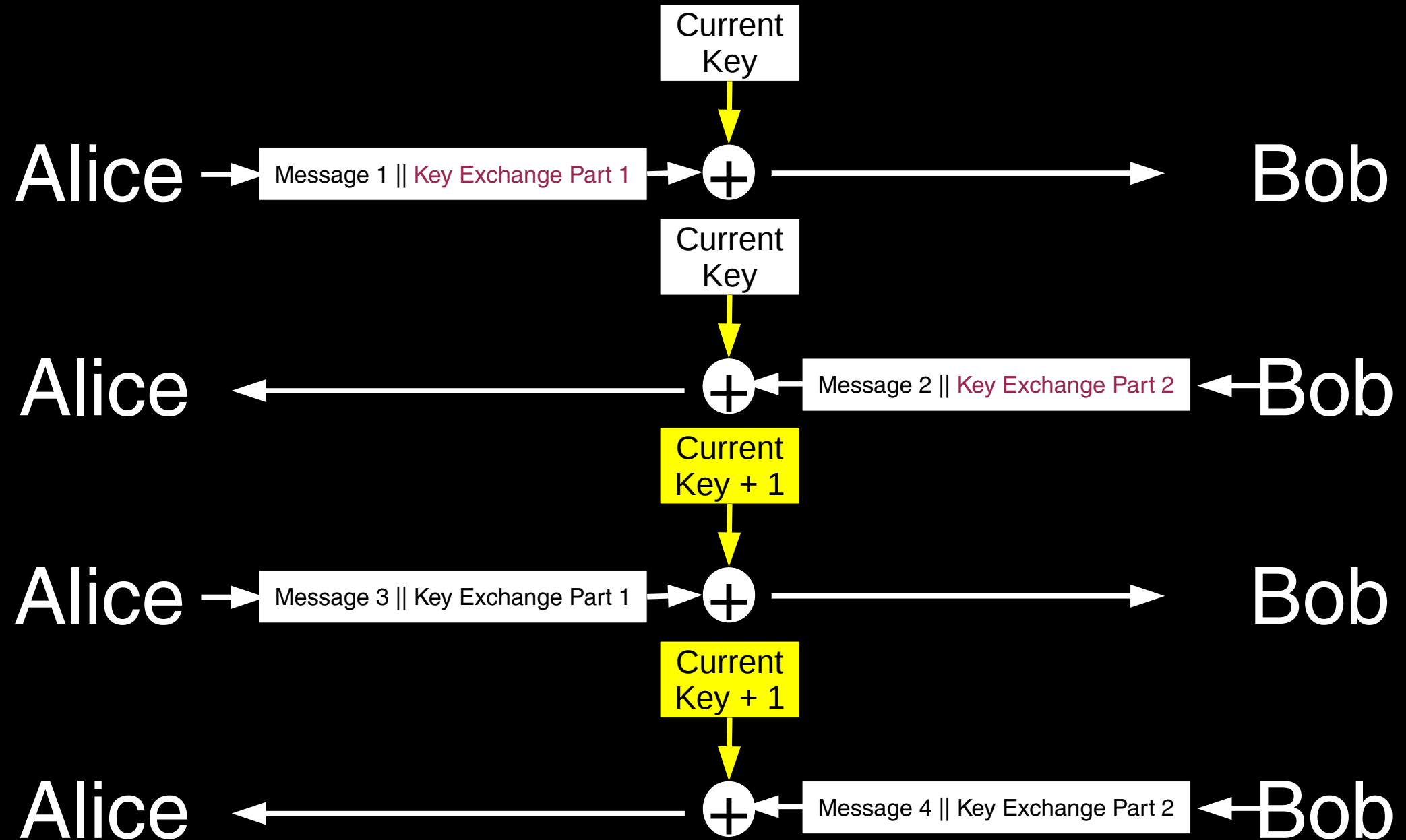
WHISPER SYSTEMS



OTR Model



OTR Model



SMALL HOPE TO REDUCE CHOICE SCOPE

WWW.THUGHTCRIME.ORG
MOXIE@THOUGHTCRIME.ORG